高中数学竞赛专题讲座

丛书策划 李胜宏
丛书主编 陶平生 苏建一
刘康宁 边红平

C H U D E N G S H U L U N

初等数论

本书主编 边红平

浙江大学出版社

图书在版编目(CIP)数据

高中数学竞赛专题讲座．初等数论 / 陶平生等主编.
—杭州:浙江大学出版社,2007.4
ISBN 978-7-308-05239-9

Ⅰ.高... Ⅱ.陶... Ⅲ.数学课—高中—教学参考资料
Ⅳ.G634.603

中国版本图书馆 CIP 数据核字(2007)第 039715 号

初等数论

本书主编 边红平

责任编辑 吴 慧 杨晓鸣
出版发行 浙江大学出版社
(杭州天目山路 148 号 邮政编码 310028)
(E-mail:zupress@mail.hz.zj.cn)
(网址:http://www.zjupress.com)
排 版 浙江大学出版社电脑排版中心
印 刷 杭州杭新印务有限公司
开 本 787mm×960mm 1/16
印 张 12.75
印 数 00001—10000
字 数 260 千
版 印 次 2007 年 4 月第 1 版 2007 年 4 月第 1 次印刷
书 号 ISBN 978-7-308-05239-9
定 价 16.00 元

浙江大学出版社发行部邮购电话 (0571)88072522

丛书编委会

编写说明

影响最大、级别最高的中学生“国际数学奥林匹克”(简称 IMO)由来已久,自第 1 届 IMO 于 1959 年在罗马尼亚举行以来,有近 60 年的历史,其影响越来越广泛。在国际数学奥林匹克的推动下,世界各地的数学竞赛活动如火如荼。目前,我国数学竞赛逐步形成了从全国联合竞赛、全国中学生数学冬令营到国家集训队一个完整的竞赛选拔体系。

数学竞赛作为一项智力活动,吸引了无数数学爱好者积极参与,也为那些对数学有浓厚兴趣和有数学天赋的学生提供一个展示自我的平台,是发现和培养数学人才的一条有效渠道。我们欣喜地看到,通过这项活动,发现了一批数学苗子,培养了一批数学人才。许多参与竞赛的优秀选手后来都成了杰出的数学家。

总体看来,我国的数学竞赛体制日趋完善,它的一些功能和作用也日益凸显。随着高校招生制度的改革,各种学科竞赛,尤其是数学竞赛的选拔功能越来越被广大高校所认可。事实上,学科竞赛已经成为高校自主招生和选拔人才的重要途径之一。

我们本着为数学竞赛的普及、提高做点有益事情的愿望,在全国范围内组织一批长期从事数学竞赛且做出杰出成绩的一线专家编写了一套“高中数学竞赛专题讲座丛书”。丛书包括《初等数论》、《函数与函数方程》、《复数与多项式》、《不等式》、《组合问题》、《排列组合与概率》、《数列与归纳法》、《集合与简易逻辑》、《三角函数》、《立体几何》、《平面几何》、《解析几何》和《数学结构思想及解题方法》13 种。

丛书的起点是高中阶段学生必须掌握的数学基本知识和全国数学竞赛大纲要求的一些基本数学思想、方法,凡是对数学爱好的高中学生都有能力阅读。丛书的特点是:

1.充分吸收了世界各地的优秀数学竞赛试题，通过对典型例题的解剖，传授数学思想方法，侧重培养学生的逻辑思维能力，不唯解题而解题；

2.本着少而精的原则选择材料，不搞题海战术，不追求大而全，而是以点带面，举一反三；

3.以数学修养和能力培养为立意，通过深刻剖析问题的数学背景，挖掘数学内涵，培养学生的数学品格和解决实际问题的能力；

4.在注重基础知识训练同时，作适当程度的拔高，对参加冬令营甚至是更高层次的竞赛都有一定的指导作用和参考价值。

丛书由浙江大学数学系教授、博士生导师、全国数学奥林匹克竞赛领队李胜宏策划；丛书由陶平生、苏建一、刘康宁、边红平主编；参加编写的成员是：陶平生、苏建一、刘康宁、边红平、黄军华、王建中、岑爱国、韦吉珠、张 雷、王俊明、李世杰、沈虎跃、斯理炯、虞金龙、马洪炎。

鉴于我们的水平有限，书中的不妥之处敬请读者批评指正。

目 录

第一章 整 除

§1.1 整除与余数

知识扫描

1. 整数的离散性 任何两个整数 x,y 之间的距离至少为 1,因此有不等式 $x<y\Leftrightarrow x+1\leqslant y$.

2. 整数的奇偶性 将全体整数分为两类,凡是 2 的倍数的数称为偶数,否则称为奇数.因此,任一偶数可表示为 $2m(m\in\mathbf{Z})$的形式,任一奇数可表示为 $2m+1$ 或 $2m-1$ 的形式.奇、偶数具有如下性质:(1)奇数±奇数=偶数;偶数±偶数=偶数;奇数±偶数=奇数;偶数×偶数=偶数;奇数×偶数=偶数;奇数×奇数=奇数.(2)奇数的平方都可以表示为 $8m+1$ 的形式,偶数的平方都可以表示成 $8m$ 或 $8m+4$ 的形式($m\in\mathbf{Z}$).(3)任何一个正整数 n,都可以写成 $n=2^m l$ 的形式,其中 m 为非负整数,l 为奇数.

3. 整数的整除性 (1)若 $a|b,b|c$,则 $a|c$.(2)若 $a|b_i$,则 $a|\sum_{i=1}^{n}c_ib_i$,其中 $c_i\in\mathbf{Z},i=1,2,\cdots,n$.(3)若 $a|c,b\neq0$,则 $ab|cb$,反之亦成立.(4)若 $a|b$,则 $|a|\leqslant|b|$.因此,若 $a|b$,又 $b|a$,则 $a=\pm b$.(5)a、b 互质,若 $a|c,b|c$,则 $ab|c$.(6)p 为质数,若 $p|a_1a_2a_3\cdots a_n$,则 p 必能整除 $a_1,a_2,\cdots,a_n$ 中的某一个.(7)如果在等式 $\sum_{i=1}^{n}a_i=\sum_{k=1}^{m}b_k$ 中除开某一项外,其余各项都是 c 的倍数,则这一项也是 c 的倍数.(8)n 个连续整数中有且仅有一个是 n 的倍数.(9)任意 n 个连续整数之积一定是 $n!$ 的倍数.

4. **带余除法** 设 a,b 为整数，$b>0$，则存在整数 q 和 r，使得 $a=bq+r$，其中

$$0\leqslant r<b, \tag{①}$$

并且整数 q 和 r 由上述条件唯一确定.

实际上，取 bq 是不超过 a 的 b 之最大倍数，即整数 q 满足 $bq\leqslant a<b(q+1)$，令 $r=a-bq$，则自然有 $0\leqslant r<b$. 于是我们得出了一个形如①式的表示. 如果还有整数 q_1 和 r_1，使 $a=bq_1+r_1$，且 $0\leqslant r_1<b$，则由①得出 $b(q-q_1)=r_1-r$，于是 $b\mid(r-r_1)$，但 $0\leqslant|r-r_1|<b$，故必须 $r-r_1=0$，即 $r=r_1$，于是 $q=q_1$，这就证明了所说的唯一性.

5. **整数的尾数函数的性质** 整数 a 的个位数也称为整数 a 的尾数，并记为 $G(a)$，$G(a)$ 也称为尾数函数，它有以下性质：

(1) $G(G(a))=G(a)$.

(2) $G(a+b+\cdots+c)=G(G(a)+G(b)+\cdots+G(c))$.

(3) $G(a\cdot b\cdot\cdots\cdot c)=G(G(a)\cdot G(b)\cdot\cdots\cdot G(c))$. 特别地，$G(a^n)=G(G^n(a))$.

(4) $G(10a)=0$，$G(10a+b)=G(b)$.

(5) 若 $a-b=10c$，则 $G(a)=G(b)$.

(6) $G(a^{4k})=G(a^4)$，$a,k\in\mathbf{N}_+$.

(7) $G(a^{4k+r})=G(a^r)$，$k\geqslant0$，$0<r<4$，$a,k,r\in\mathbf{N}_+$.

(8) $G\left(a^{b_1^{b_2^{\cdot^{\cdot^{\cdot^{b_n}}}}}}\right)=\begin{cases}G(a)\text{（当 } b_1 \text{ 为奇数，} b_2 \text{ 为偶数时）；}\\ G(a^4)\text{（当 } b_1 \text{ 为偶数，} b_2 \text{ 为奇数或 } b_1 \text{ 为偶数，} b_2 \text{ 为偶数时）；}\\ G(a^{b_1})\text{（当 } b_1 \text{ 为奇数，} b_2 \text{ 为奇数时）.}\end{cases}$

例题分析

例 1 求 $a、b、c$，使它们满足不等式 $a^2+b^2+c^2+3<ab+3b+2c(a,b,c\in\mathbf{Z})$.

分析 利用整数的离散性及配方法.

解 由题意，整数 a,b,c 满足 $a^2+b^2+c^2+3<ab+3b+2c$，

即 $a^2+b^2+c^2+4\leqslant ab+3b+2c$.

配方得 $\left(a-\dfrac{b}{2}\right)^2+3\left(\dfrac{b}{2}-1\right)^2+(c-1)^2\leqslant0$.

由于 $\left(a-\dfrac{b}{2}\right)^2\geqslant0$，$\left(\dfrac{b}{2}-1\right)^2\geqslant0$，$(c-1)^2\geqslant0$，

故有 $a-\dfrac{b}{2}=\dfrac{b}{2}-1=c-1=0$，

即 $a=1,b=2,c=1$.

例 2 设 $F_k=2^{2^k}+1$，$k\geqslant 0$. 证明：若 $m>n$，则 $F_n\mid(F_m-2)$.

分析 题目所证的式子为 $2^{2^n}+1\mid 2^{2^m}-1$，应联想到先证明 $2^{2^{n+1}}-1\mid 2^{2^m}-1$，再利用 $2^{2^{n+1}}-1=(2^{2^n}-1)\cdot(2^{2^n}+1)$，证明原命题.

证明 首先将 x^k-y^k 分解因式，即

$x^k-y^k=(x-y)\cdot(x^{k-1}+x^{k-2}y+\cdots+xy^{k-2}+y^{k-1})$ ①

在上式中，取 $x=2^{2^{n+1}}$，$y=1$，$k=2^{m-n-1}$，得

$2^{2^m}-1=(2^{2^{n+1}}-1)\cdot(x^{k-1}+x^{k-2}y+\cdots+xy^{k-2}+y^{k-1})$，

得到 $2^{2^{n+1}}-1\mid 2^{2^m}-1$.

又 $2^{2^{n+1}}-1=(2^{2^n}+1)\cdot(2^{2^n}-1)$，故可得 $2^{2^n}+1\mid 2^{2^m}-1$.

例 3 设 n 为奇数，证明：$n\mid\left(1+\frac{1}{2}+\cdots+\frac{1}{n-1}\right)\cdot(n-1)!$.

分析 由于 $1+\frac{1}{n-1}=\frac{n}{n-1}$，$\frac{1}{2}+\frac{1}{n-2}=\frac{n}{2(n-2)}$，…，这些数的分子都是 n，分母都小于 $(n-1)!$，故而应该想到用配对法做此题.

证明 由于 $\left(\frac{1}{k}+\frac{1}{n-k}\right)\cdot(n-1)!=\frac{n}{k(n-k)}\cdot(n-1)!$，$1\leqslant k\leqslant n-1$，

其中 $k(n-k)\mid(n-1)!$，故有 $n\mid\frac{n}{k(n-k)}\cdot(n-1)!$.

所以设 $n=2m+1$，$m\geqslant 0$，

则 $\left(1+\frac{1}{2}+\cdots+\frac{1}{n-1}\right)\cdot(n-1)!=\left(1+\frac{1}{2}+\cdots+\frac{1}{2m}\right)\cdot(n-1)!$

$=\left[\left(1+\frac{1}{2m}\right)+\left(\frac{1}{2}+\frac{1}{2m-1}\right)+\cdots+\left(\frac{1}{m}+\frac{1}{m+1}\right)\right]\cdot(n-1)!$

$=\left[\frac{2m+1}{2m}+\frac{2m+1}{2(2m-1)}+\cdots+\frac{2m+1}{m(m+1)}\right]\cdot(n-1)!$

$=\left[\frac{n}{(n-1)}+\frac{n}{2(n-2)}+\cdots+\frac{n}{\left(n-\frac{n-1}{2}\right)\left(n-\frac{n-3}{2}\right)}\right]\cdot(n-1)!$

显然，$(n-1)\mid(n-1)!$，$2(n-2)\mid(n-1)!$，…，$\left(n-\frac{n-1}{2}\right)\left(n-\frac{n-3}{2}\right)\mid(n-1)!$，

所以，$n\mid\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n-1}\right)\cdot(n-1)!$.

例 4 设 m,n 为正整数，$m>2$，证明：$(2^m-1)\nmid(2^n+1)$.

分析与证明 (1) $n<m$ 时 $(m>2)$，显然有 $2^m-1>2^n+1$，

故此时 $2^m-1\nmid 2^n+1$.

(2) 当 $n=m$ 时，

由于 $2^n+1<2^{m+1}-2$，故 $1<\frac{2^n+1}{2^m-1}<2$，

所以此时 $2^m-1\nmid 2^n+1$.

(3)当 $n>m$ 时，可以用带余除法转换到上述特殊情形.

设 $n=mq+r$，$0\leqslant r<m$，而 $q\geqslant 0$，

由于 $2^n+1=(2^{mq}-1)2^r+2^r+1$，

而$(2^m-1)|(2^{mq}-1)$，$(2^m-1)\nmid(2^r+1)$（因 $0\leqslant r<m$），

从而当 $n>m$ 时有 $2^m-1\nmid 2^n+1$.

综合(1)，(2)，(3)得 $2^m-1\nmid 2^n+1$.

例 5 设 ax_0+by_0 是形如 $ax+by$（a,b 不全为零）的整数中最小的正数，试证明：对任意整数 x,y 恒有 $ax_0+by_0|ax+by$.

分析与证明 对任意整数 x,y 存在唯一的 q,r，使 $ax+by=(ax_0+by_0)q+r$，$0\leqslant r<ax_0+by_0$.

若 $r\neq 0$，则 $0<r<ax_0+by_0$，且 $r=a(x-x_0q)+b(y-y_0q)$，

而 $x-x_0q$ 与 $y-y_0q$ 均为整数，

故 r 是一个比 ax_0+by_0 还要小的形如 $ax+by$ 的正整数.

这与 ax_0+by_0 的最小性相矛盾.

因此，必有 $r=0$，故 $ax_0+by_0|ax+by$.

例 6 设 $n\in\mathbf{N}_+$，求证：$512|3^{2n}-32n^2+24n-1$.

分析 设 $f(n)=3^{2n}-32n^2+24n-1$，欲证 $512|f(n)$，我们可运用递推思想转而证明 $512|f(1)$，以及 $512|(f(n+1)-f(n))$，$n\in\mathbf{N}_+$.

证明 设 $f(n)=3^{2n}-32n^2+24n-1$，

因为 $f(1)=0$，则 $512|f(1)$；

又 $f(n+1)-f(n)$

$=(3^{2n+2}-32(n+1)^2+24(n+1)-1)-(3^{2n}-32n^2+24n-1)=8(3^{2n}-8n-1)$.

因为 $512=8\times 64$，故只需证明 $64|(3^{2n}-8n-1)$.

设 $g(n)=3^{2n}-8n-1$，

因为 $g(1)=0$，则 $64|g(1)$.

又 $g(n+1)-g(n)=(3^{2n+2}-8(n+1)-1)-(3^{2n}-8n-1)=8(3^{2n}-1)=8(9^n-1)$

$=8(9-1)\cdot(9^{n-1}+9^{n-2}+\cdots+1)$

$=64(9^{n-1}+9^{n-2}+\cdots+1)$.

可见，$64|(g(n+1)-g(n))$，

于是，$64|g(n)$，因此 $512|f(n)$.

例 7 证明：对于任何正整数 n 和 k，数 $f(n,k)=2n^{3k}+4n^k+10$ 都不能分解成若干

个连续的自然数之积.

分析 看到"连续的若干个正整数"就应该想到"连续的 n 个正整数之积被 $n!$ 整除".

证明 只需证明 $f(n,k)$ 不能被很小的一个正整数 n 整除即可.

由 $f(n,k)=3n^{3k}+3n^k-n^{3k}+n^k+10$

$$=3(n^{3k}+n^k+3)-n^k(n^k-1)(n^k+1)+1.$$

又因为 $3\mid 3(n^{3k}+n^k+3)$，$3\mid(n^k-1)(n^k+1)\cdot n^k$，$3\nmid 1$.

故 $3\nmid f(n,k)$，因而 $f(n,k)$ 不能分解成三个或三个以上的连续正整数的乘积.

再证明 $f(n,k)$ 不能分解成两个连续正整数的积.

由上知，$f(n,k)=3q+1(q\in \mathbf{N}_+)$，因而只需证方程 $3q+1=x(x+1)$ 无正整数解.

分别将 $x=3r,3r+1,3r+2$ 代入上述方程中，$x(x+1)$ 均不是 $3q+1$ 型的数.

故 $f(n,k)$ 对任何正整数 n,k 都不能分解成若干个连续的正整数之积.

例 8 求最大的正整数 x，使得对每一个正整数 y，都有 x 能整除 $7^y+12y-1$.

分析 由于 $7^y+12y-1$ 随 y 的增加而增加，当 $y=1$ 时，取最小值 18，因此由 $x\mid(7^y+12y-1)$，得 $x\mid 18$，故 x 是 18 的约数. 又因当 $y=2$ 时，$7^2+12\times2-1=72=18\times4$，当 $y=3$ 时，$7^3+12\times3-1=378=18\times21$，都有 $18\mid 7^y+12y-1$，故猜测符合题意的 $x=18$.

解 采用数学归纳法，当 $y=1$ 时，猜测成立. 归纳假设当 $y=k$ 时，猜测为真，即 $18\mid(7^k+12k-1)$，则当 $y=k+1$ 时，

$$7^{k+1}+12(k+1)-1=7^k+12k-1+6\times7^k+12=(7^k+12k-1)+6(7^k+2).$$

由归纳假设，知 $7^k+12k-1$ 能被 18 整除.

因此，只需证明 7^k+2 能被 3 整除.

事实上，$7^k=(6+1)^k$

$$=6^k+C_k^1\cdot6^{k-1}+C_k^2\cdot6^{k-2}+\cdots+C_k^k$$

$$=6(6^{k-1}+C_k^1\cdot6^{k-2}+C_k^2\cdot6^{k-3}+\cdots+C_k^{k-1})+1,$$

故 7^k 被 3 除余 1. 故 7^k+2 能被 3 整除.

因此，由 $y=k+1$ 时，$18\mid(7^{k+1}+12(k+1)-1)$，从而用归纳法证明了此题.

例 9 证明存在无穷多个正整数 n，使得 $n\mid 2^n+2$，$n-1\mid 2^n+1$.

分析 处理无穷这类问题，大致上有两种方法：其一是反证法，即假设只有有限多个，能使其导出矛盾；其二是构造法，可构造出"无穷"多个自然数满足题中要求. 本题采用构造法.

证明 显然，$2\mid 2^2+2$，$(2-1)\mid 2^2+1$，

假设存在 $n\in\mathbf{N}_+$，使 $n\mid 2^n+2$，$n-1\mid 2^n+1$，

由于 $n\mid 2^n+2$，知 $2\mid n$，$4\nmid n$.

由 $n-1 | 2^n+1$，知存在 $k\in\mathbf{N}_+$，使 $2^n+1=(n-1)k$，其中，$2\nmid(n-1)$，$2\nmid k$.

故 $2^{2^n+1}+1=2^{(n-1)k}+1=(2^{n-1}+1)m, m\in\mathbf{N}_+$，

于是 $2^{n-1}+1 | 2^{2^n+1}+1$.

对此式两边同乘以 2，则有 $(2^n+2) | (2^{2^n+2}+2)$.

由于 $n | 2^n+2$，$4\nmid n$，则 $2^n+2=nt$，t 为奇数，$2^{2^n+2}+1=2^{nt}+1=(2^n+1)s, s\in\mathbf{N}_+$，

即有 $2^n+1 | 2^{2^n+2}+1$.

于是，当 $n | 2^n+2$，$(n-1) | 2^n+1$，$2 | n$，$4\nmid n$ 时，必有 $2^n+2 | 2^{2^n+2}+2$，且 $(2^n+1) | (2^{2^n+2}+1)$.

因此，由 $n=2$ 可生成 $2^2+2=6$，$2^6+2=66$，$2^{66}+2$，…. 如此下去，可以得到无穷多个符合题目要求的正整数 n.

例 10　试求出所有的正整数 a,b,c，其中 $1<a<b<c$，且使得 $(a-1)(b-1)(c-1)$ 是 $abc-1$ 的约数.

分析与解　依题意，存在 $k\in\mathbf{N}$，使

$$abc-1=k(a-1)(b-1)(c-1) \qquad ①$$

由整数的离散性，有 $a\leqslant b-1$，$a\leqslant c-2$，

故 $(k-1)(a-1)(b-1)(c-1)=(abc-1)-(a-1)(b-1)(c-1)$

$=ab+bc+ca-a-b-c=a(b-1)+b(c-1)+c(a-1)$

$\leqslant(c-2)(b-1)+b(c-1)+c(b-2)=3(bc-b-c+1)-1$

$<3(b-1)(c-1)$，

所以 $(k-1)(a-1)<3$.

又因为 $a(b-1)+b(c-1)+c(a-1)>0$，

所以 $k\neq1$，故有 $(k-1)\cdot(a-1)=1$ 或 $(k-1)(a-1)=2$.

(1)若 $(k-1)(a-1)=1$ 成立，则 $k=a=2$.

这时，①式左边为奇，右边为偶，矛盾.

(2)若 $(k-1)(a-1)=2$ 成立，则 $a=3,k=2$ ②

或 $a=2,k=3$ ③

将②代入①，得 $3bc-1=4(b-1)(c-1)=4(bc-b-c+1)$，

即 $bc-4(b+c)+16=11$，即 $(b-4)(c-4)=11$.

又由 $c>b$，得 $b-4=1$，$c-4=11$，

所以 $b=5$，$c=15$.

同样，将③代入①中可求得 $b=4$，$c=8$.

经检验，得 $a=3,b=5,c=15$，或 $a=2,b=4,c=8$.

例 11　设 p 是质数，整数 x、y、z 满足 $0<x<y<z<p$，若 x^3、y^3、z^3 除以 p 的余数相

等，证明：$x^2+y^2+z^2$ 可以被 $x+y+z$ 整除.

分析 由 $0<x<y<z<p$，及 x^3、y^3、z^3 除以 p 的余数相等这两个条件中挖掘出 x、y、z 与 p 的关系，如 $p|(x^3-y^3)$，等等. 利用这些关系，分别可以推导出 p 与 $x+y+z$，p 与 $x^2+y^2+z^2$ 之间的整除关系，进而得出 $(x+y+z)|(x^2+y^2+z^2)$.

证明 由已知条件 x^3、y^3、z^3 除以 p 的余数相等，

可得 $p|(x^3-y^3)$，即 $p|(x-y)(x^2+xy+y^2)$.

由于 $0<x<y<p$，p 为质数，故 $|x-y|<p$. 故 $p\nmid|x-y|$.

因此，$p|(x^2+xy+y^2)$. ①

同理可得，$p|(y^2+yz+z^2)$， ②

$p|(x^2+xz+z^2)$， ③

由①、②知 $p|[(x^2+xy+y^2)-(y^2+yz+z^2)]$

即 $p|(x-z)(x+y+z)$.

同上面一样可证明 $p\nmid(x-z)$. 所以 $p|(x+y+z)$.

已知 $0<x<y<z<p$，所以 $x+y+z=p$ 或 $2p$.

由 $p>3$，则 $(2,p)=1$，

而 $x+y+z$ 和 $x^2+y^2+z^2$ 除以 2 的余数相同. 故只须证 $p|(x^2+y^2+z^2)$，

由①得 $p|[x(x+y+z)+y^2-xz]$，

于是，$p|y^2-xz$， ④

同理，$p|x^2-yz$， ⑤

$p|z^2-xy$. ⑥

再由①－⑥可得 $p|3(x^2+y^2+z^2)$，所以 $p|(x^2+y^2+z^2)$.

故 $(x+y+z)|(x^2+y^2+z^2)$.

能力训练

1. 设 a，b，c，d 为整数，$(a-c)|(ab+cd)$，则 $(a-c)|(ad+bc)$.

2. 设 a，b 都是正整数，a^2+ab+1 被 b^2+ab+1 整除，证明：$a=b$.

3. 在已知数列 1，4，8，10，16，19，21，25，30，43 中，相邻若干个数之和能被 11 整除的数组共有多少组？

4.（第 32 届美国数学奥林匹克）证明：对每个正整数 n，存在一个可以被 5^n 整除的 n 位正整数，它的每一位上的数字都是奇数.

5. 求证：将任给的 12 个不同正整数用适当运算符号（如＋、－、×、÷）连结起来，所

得的结果一定有 20790 的倍数.

6. 设 a、b、c、d 为奇数，$0<a<b<c<d$，且 $ad=bc$，$a+d=2^k$，$b+c=2^m$，k，m 为整数，求 a 的值.

7. 设 a，m，n 都是正整数，$a>1$，且 $(a^m+1)\mid(a^n+1)$，证明：$m\mid n$.

8.（第 20 届伊朗数学奥林匹克）已知数列 $\{a_n\}$，且 $a_0=2$，$a_1=1$，$a_{n+1}=a_n+a_{n-1}$，证明：若 p 是 $a_{2k}-2$ 的质因子，则 p 也是 $(a_{2k+1}-1)$ 的质因子.

9. 设 $x_1,x_2,\cdots,x_n,y_1,y_2,\cdots,y_n,z_1,z_2,\cdots,z_n$ 都是 1 或 -1，且 $x_1y_1+x_2y_2+\cdots+x_ny_n=0$，$x_1z_1+x_2z_2+\cdots+x_nz_n=0$，$y_1z_1+y_2z_2+\cdots+y_nz_n=0$，求 n 的值.

10. 将前 $2n$ 个自然数随意写成一行，并依次编号为 $1,2,\cdots,2n$，然后求出每个数与它的号数之和，得到 $2n$ 个和数，再用 $2n$ 分别去除每一个和数，得 $2n$ 个商及余数，求证：至少有两个余数相同.

11. 设 a、b 是大于 1 的正整数，$(a,b)=1$，证明：有唯一一对整数 r，s，满足 $ar-bs=1$，且 $0<r<b$，$0<s<a$.

12. 哪些连续正整数之和为 6^3？求出所有解.

13.（2005 年意大利数学奥林匹克）证明：在任意 18 个连续的且小于或等于 2005 的正整数中，至少存在一个整数能被其各位数字之和整除.

14.（2005 年保加利亚国家数学奥林匹克）设 a、b、c 是正整数，且 $ab\mid c(c^2-c+1)$，$(c^2+1)\mid(a+b)$. 证明：a、b 中有一个数等于 c，另一个数等于 c^2-c+1.

15.（2005 年克罗地亚国家数学竞赛）求所有可用十进制表示为 $\overline{13xy45z}$，且能被 792 整除的正整数，其中 x、y、z 为未知数.

§1.2　最大公因数和最小公倍数

知识扫描

1. 欧几里得算法　设 a，b 为整数，$b>0$，按下述方式反复作带余除法，有限步之后必然停止（即余数为零）：

$$\begin{cases}\text{用 } b \text{ 除 } a: a=bq_0+r_0, 0<r_0<b;\\ \text{用 } r_0 \text{ 除 } b: b=r_0q_1+r_1, 0<r_1<r_0;\\ \text{用 } r_1 \text{ 除 } r_0: r_0=r_1q_2+r_2, 0<r_2<r_1;\\ \cdots\\ \text{用 } r_{n-1} \text{ 除 } r_{n-2}: r_{n-2}=r_{n-1}q_n+r_n, 0<r_n<r_{n-1};\\ \text{用 } r_n \text{ 除 } r_{n-1}: r_{n-1}=r_nq_{n+1}+r_{n+1}, r_{n+1}=0;\end{cases} \quad ①$$

则$(a,b)=(r_0,b)=(r_1,r_0)=\cdots=(r_{n+1},r_n)=r_n$.

实际上，由于余数 $r_0,r_1,\cdots$为整数，且满足 $r_0>r_1>\cdots>r_{n-1}>\cdots\geqslant 0$，

从而上述的带余除法有限步后余数必为零.

2. 裴蜀等式　设 a,b 是整数，且 $d\mid(a,b)$，则$(a,b)=d$ 的充要条件是存在整数 u,v，使得 $ua+vb=d$.

给定 a,b，欧氏算法不仅能（在有限步内）求出(a,b)，还可证明方程

$$ua+vb=(a,b) \quad ②$$

有一组解 u,v，并能实际地求出一组解. 具体做法是将欧氏算法倒推回去：由①中倒数第二行得$(a,b)=r_n=r_{n-2}-r_{n-1}q_n$，这就将$(a,b)$表示成"$r_{n-1}\times$整数$+r_{n-2}\times$整数"的形式；用①中倒数第三行 $r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}$代入上式，消去 r_{n-1}，得出$(a,b)=r_{n-2}(1+q_{n-1}q_n)-r_{n-3}q_n$，即$(a,b)$表示成"$r_{n-2}\times$整数$+r_{n-3}\times$整数"的形式；如此进行，最终便求得②中一组解 u,v.

3. 最大公约数和最小公倍数的定义及性质　设 $a,b,\cdots,c$ 是（有限个）不全为零的整数，则同时除尽 $a,b,\cdots,c$ 的整数（如±1）叫做它们的公约数（或公因子）. 非零整数的约数有有限个，故 $a,b,\cdots,c$ 的公约数有有限个. 其中必有一个最大的，我们称它为 $a,b,\cdots,c$ 的最大公约数.

同样的，任一个为所有 $a,b,\cdots,c$ 的倍数的数称为它们的公倍数，最小的正的公倍数叫做最小公倍数，记为$[a,b,\cdots,c]$.

下面介绍最大公约数和最小公倍数的一些性质.

(1)a 和 b 的任一公约数都是它们最大公约数的约数；

(2)$m\in\mathbf{N}$，则$(am,bm)=m(a,b)$；

(3)设 c 为 a,b 的公约数，则$\left(\frac{a}{c},\frac{b}{c}\right)=\frac{(a,b)}{c}$，特别地，若 $c=(a,b)$，则$\left(\frac{a}{c},\frac{b}{c}\right)=1$；

(4)设 $a_1,a_2,\cdots,a_n$ 是任意 n 个正整数，如果$(a_1,a_2)=c_2$，$(c_2,a_3)=c_3$，$\cdots$，$(c_{n-1},a_n)=c_n$，则$(a_1,a_2,\cdots,a_n)=c_n$；

(5)设 a 和 b 均与 m 互素，则 ab 也与 m 互素，即与 m 互素的整数关于乘法封闭，一般地，如果 $a_1,a_2,\cdots,a_n$ 均与 m 互素，则 $a_1a_2a_3\cdots a_n$ 与 m 互素；

(6)若 $b|ac$,$(b,c)=1$,则 $b|a$;

(7)若$(a,b)=1$,则$(ac,b)=(c,b)$;

(8)若 m 是整数,$a|m$,$b|m$,则$[a,b]|m$,即 a,b 的任一公倍数是其最小公倍数的倍数;

(9)若 m 是正整数,则 $m[a,b]=[ma,mb]$;

(10)$(a,b)[a,b]=|ab|$,特别地,若$(a,b)=1$,则$[a,b]=|ab|$;

(11)设 $b_1,b_2,\cdots,b_n$ 是两两互素的正整数,a 是任意整数,若 $b_i|a(i=1,2,\cdots,n)$,则 $b_1b_2\cdots b_n|a$,因此特别地,两两互素的正整数的最小公倍数等于它们的乘积;

(12)设 $a_1,a_2,\cdots,a_n$ 是任意 n 个正整数,若$[a_1,a_2]=m_2$,$[m_2,a_3]=m_3$,$\cdots$,$[m_{n-1},a_n]=m_n$,则$[a_1,a_2,\cdots,a_n]=m_n$.

例题分析

例 1 (1)设 n 是正整数,证明:$(21n+4,14n+3)=1$;(2)证明:$(n!+1,(n+1)!+1)=1$;(3)记 $F_k=2^{2^k}+1$,$k\geqslant 0$,证明:对 $m\neq n$,有$(F_m,F_n)=1$.

分析 (1)、(2)只需用欧式算法即可,(3)要联立裴蜀等式.

证明 (1)由欧氏算法,得

$$\begin{aligned}(21n+4,14n+3)&=(21n+4-14n-3,14n+3)\\&=(7n+1,14n+3)=(7n+1,14n+3-2(7n+1))\\&=(7n+1,1)=1.\end{aligned}$$

(2)由于$(n+1,(n+1)!+1)=1$,

$$\begin{aligned}\text{所以}(n!+1,(n+1)!+1)&=((n!+1)(n+1),(n+1)!+1)\\&=((n!+1)(n+1)-(n+1)!-1,(n+1)!+1)\\&=(n,(n+1)!+1).\end{aligned}$$

设 d 为 $n!+1$ 与$(n+1)!+1$ 的最大公约数,

由上式,知 $d|n$,即 $d|n!$.

又因为 $d|(n!+1)$,所以,$d=1$.

即$(n!+1,(n+1)!+1)=1$.

(3)由上一节例 2 可知,对于 $m>n$,

有 $F_n|(F_m-2)$,

即存在整数 x 使 $F_m-2=xF_n$,

即 $F_m-x\cdot F_n=2$.

设 $d=(F_m,F_n)$，由 $F_m-xF_n=2$ 推出 $d|2$，所以 $d=1$ 或 2，但 F_n 显然是奇数.

所以 $d=1$，即 $(F_m,F_n)=1$.

例 2 设 k 为正奇数，证明：$\frac{n(n+1)}{2}|(1^k+2^k+\cdots+n^k)$.

分析 因为 $(n,n+1)=1$，故可考虑分别证明 $n|2(1^k+2^k+\cdots+n^k)$，$(n+1)|2(1^k+2^k+\cdots+n^k)$.

证明 问题等价于证明 $n(n+1)|2(1^k+2^k+\cdots+n^k)$.

对于正整数 x,y，有

$x^k+y^k=(x+y)(x^{k-1}-x^{k-2}y+\cdots+(-1)^{k-2}xy^{k-2}+(-1)^{k-1}y^{k-1})$，

则 $(x+y)|(x^k+y^k)$，

所以由 $2(1^k+2^k+\cdots+n^k)$

$$=(1^k+(n-1)^k)+(2^k+(n-2)^k)+\cdots+((n-1)^k+1^k)+2n^k,$$

可知 $n|2(1^k+2^k+\cdots+n^k)$.

同样，由 $2(1^k+2^k+\cdots+n^k)=(1^k+n^k)+(2^k+(n-1)^k)+\cdots+(n^k+1^k)$，

可知 $(n+1)|2(1^k+2^k+\cdots+n^k)$，

又 $(n,n+1)=1$，则 $n(n+1)|2(1^k+2^k+\cdots+n^k)$，

即 $\frac{n(n+1)}{2}|(1^k+2^k+\cdots+n^k)$.

例 3 数列 1001，1004，1009 的通项是 $a_n=n^2+1000$，其中 $n\in\mathbf{N}_+$. 对于每一个 n，用 d_n 表示 a_n 与 a_{n+1} 的最大公约数，求 d_n 的最大值，其中 n 取一切正整数.

分析与解 设 $d_n=(1000+n^2,1000+(n+1)^2)$，则 $d_n|(1000+n^2)$，$d_n|(1000+(n+1)^2)$. 所以 $d_n|(1000+(n+1)^2-1000-n^2)$，

即 $d_n|(2n+1)$.

又因为 $2(1000+n^2)=n(2n+1)+2000-n$，

所以 $d_n|(2000-n)$，$d_n|((2n+1)+2(2000-n))$，即 $d_n|4001$.

所以 $1\leqslant d_n\leqslant 4001$.

又当 $n=2000$ 时，有 $1000+n^2=1000+(2000)^2=1000\cdot 4001$，$1000+(n+1)^2=1000+(2000+1)^2=1001\cdot 4001$，

所以 d_n 能得到 4001，即 $(d_n)_{\max}=4001$.

例 4 正整数 $a_1,a_2,\cdots,a_{49}$ 的和为 999，令 d 为 $a_1,a_2,\cdots,a_{49}$ 的最大公约数，问 d 的最大值为多少？

分析 由 $a_i\geqslant d$，$(i=1,2,\cdots,49)$ 以及 d 是 999 的约数，可以确定 d 的取值范围，逐一检验排除后即可得到符合题意的 d.

解 由于 $d=(a_1,a_2,\cdots,a_{49})$，则 $d|(a_1+a_2+\cdots+a_{49})$，即 $d|999$，

故 d 是 $999=3^3\cdot 37$ 的约数.

又因为 $d|a_k$，$k=1,2,\cdots,49$，则 $a_k\geqslant d$，

于是必有 $999=a_1+a_2+\cdots+a_{49}\geqslant 49d$，得到 $d\leqslant\frac{999}{49}<21$.

又由 d 是 999 的约数可知 d 只能是 1，3，9.

又因为 999 能写成 49 个数的和：$\underbrace{9+9+9+\cdots+9}_{48个9}+567=999$.

其中每一个数都能被 9 整除，所以 d 的最大值为 9.

例 5 设 $S_n=\sum\limits_{k=1}^{n}(k^5+k^7)$，求 S_n 与 S_{3n} 的最大公约数.

分析与解 由于 $S_1=1^5+1^7=2$，

$S_2=(1^5+1^7)+(2^5+2^7)=2\cdot 81=2\cdot(1+2)^4$，

$S_3=2\cdot 3^4+3^5+3^7=2\cdot 6^4=2\cdot(1+2+3)^4$，

$S_4=2\cdot 6^4+4^5+4^7=2^5\cdot 5^4=2\cdot(1+2+3+4)^4$.

由此猜想 $S_n=2(1+2+\cdots+n)^4$. ①

下面用数学归纳法证明.

$n=1$ 时，显然成立.

假设 $n=k$ 时，①式成立.

对于 $n=k+1$ 时，

$$
\begin{aligned}
S_{k+1}&=2(1+2+\cdots+k)^4+(k+1)^5+(k+1)^7\\
&=\frac{1}{8}k^4(k+1)^4+(k+1)^5+(k+1)^7\\
&=\frac{1}{8}(k+1)^4[k^4+8(k+1)+8(k+1)^3]\\
&=\frac{1}{8}(k+1)^4(k+2)^4\\
&=2[1+2+\cdots+k+(k+1)]^4.
\end{aligned}
$$

所以 $n=k+1$ 时，①式成立.

于是对所有自然数 n，①式成立.

因此，$S_n=2\left[\frac{n(n+1)}{2}\right]^4$，$S_{3n}=2\left[\frac{3n(3n+1)}{2}\right]^4$.

(1) 当 $n=2k$ 时，

$$
\begin{aligned}
d&=(S_n,S_{3n})\\
&=\left(2\left[\frac{2k(2k+1)}{2}\right]^4,2\left[\frac{6k(6k+1)}{2}\right]^4\right)\\
&=(2k^4(2k+1)^4,2\cdot 81k^4(6k+1)^4).
\end{aligned}
$$

因为$(2k+1,6k+1)=1$，所以$d=2k^4((2k+1)^4,81)$，

当$k=3t+1$时，$(2k+1)^4=(6t+3)^4=81(2t+1)^4$，

所以$d=2\cdot 81k^4=2\cdot 81\cdot \frac{n^4}{2^4}=\frac{81}{8}n^4$.

当$k\neq 3t+1$时，$d=2k^4=\frac{n^4}{8}$.

(2)当$n=2k+1$时，

$S_n=2[(2k+1)(k+1)]^4$，$S_{3n}=2[3(2k+1)(3k+2)]^4$.

因为$(3k+2,2k+1)=1$，$(3k+2,k+1)=1$，所以$d=2(2k+1)^4(3^4,(k+1)^4)$，

当$k=3t+2$时，$k+1=3(t+1)$，所以$d=2n^4\cdot 3^4=162n^4$.

当$k\neq 3t+2$时，$d=2n^4$.

例6 正整数a和b互素，证明：$a+b$与a^2+b^2的最大公约数等于1或2.

分析 设d为$a+b$和a^2+b^2的最大公约数，由于$(a+b)^2-(a^2+b^2)=2ab$及$2a(a+b)-2ab=2a^2$，可知$d|2a^2$，及$d|2b^2$，再由$(a,b)=1$，可证得本题.

证明 设d是a^2+b^2及$a+b$的最大公约数，

则有$d|(a^2+b^2)$，$d|(a+b)$，

于是由$(a+b)^2-(a^2+b^2)=2ab$，得$d|2ab$.

又因为$2a(a+b)-2ab=2a^2$，$2b(a+b)-2ab=2b^2$.

所以$d|2a^2$，$d|2b^2$，

因此，d是$2a^2$和$2b^2$的公约数.

由题设，$(a,b)=1$，则有$(a^2,b^2)=1$，

所以$2a^2$和$2b^2$不可能被大于2的数整除.

因而$d\leqslant 2$.

即$a+b$与a^2+b^2的最大公约数是1或2.

例7 两数之和为667，它们的最小公倍数除以最大公约数所得的商等于120，求这两数.

分析 遇到这类最大公约数与最小公倍数有等式关系时，一般设题目中两数为x，y，d为x，y的最大公约数，$x=dx_1$，$y=dy_1$，最小公倍数为dx_1y_1，则可建立关于d、x_1、y_1的方程，从而解出x、y.

解 设所求的数为x和y，且$d=(x,y)$，

则$x=dx_1$，$y=dy_1$，$(x_1,y_1)=1$，

于是$[x,y]=\frac{xy}{d}=dx_1y_1$，

由题意，有$d(x_1+y_1)=667$， ①

$$\frac{dx_1y_1}{d}=120,\quad ②$$

由 $x_1y_1=120=2^3\cdot3\cdot5$，又 $667=1\cdot23\cdot29$，

因此由①，②可得 $x_1=8,y_1=15$，或 $x_2=24,y_2=5$，

相应地 $d_1=29,d_2=23$，

因此，所求的数有两组

$x_1=232,y_1=435$ 或 $x_2=552,y_2=115$.

例 8 设$[r,s]$表示正整数 r 和 s 的最小公倍数，求有序三元正整数组(a,b,c)的个数，其中，$[a,b]=1000,[b,c]=2000,[c,a]=2000$.

解 由$[a,b]=1000,[b,c]=2000,[c,a]=2000$ 知 a,b,c 均为 $2^m\cdot5^n$ 型的数.

不妨设 $a=2^{m_1}\cdot5^{n_1},b=2^{m_2}\cdot5^{n_2},c=2^{m_3}\cdot5^{n_3}$.

由$[a,b]=2^3\cdot5^3,[b,c]=[c,a]=2^4\cdot5^3$ 及最小公倍数的性质可知.

$\max\{m_1,m_2\}=3,\max\{m_2,m_3\}=4$,

$\max\{m_3,m_1\}=4,\max\{n_1,n_2\}=3$,

$\max\{n_2,n_3\}=3,\max\{n_3,n_1\}=3$.

由此可知，$m_3=4$，m_1 和 m_2 中必有一个是 3，此时，另一个可取 0，1，2 或 3.

不计重复，一共有 7 种不同情况.

从而满足本题条件的数组(a,b,c)共有 $7\times10=70$ 个.

例 9 用(m,n)表示正整数 m 和 n 的最大公约数，若在各项都是正整数的数列$\{a_i\}$中，对于任何 $j\neq i$，都有$(a_i,a_j)=(i,j)$，证明对一切 $i\in\mathbf{N}$，都有 $a_i=i$.

分析 首先，将 $j=ki,k\in\mathbf{Z}$ 代入题中可得到 $i|a_i$，则只需证明 $a_i>i$ 不成立即可.

证明 由题设，对每一个 a_i 都有$(a_i,a_{2i})=(i,2i)=i$，即 $i|a_i$.

下面证明 $a_i=i$.

若 $a_i>i$，一方面有$(a_{a_i},a_i)=(a_i,i)=i$.

另一方面，有$(a_{a_i},a_i)=a_i>i$.

上面两个式子相矛盾！于是只能有 $a_i=i$.

例 10 若 $n,a_1,a_2,\cdots,a_k$ 是整数，$n\geqslant a_1>\cdots>a_k>0$，且对于所有的 i 和 j，a_i 和 a_j 的最小公倍数不超过 n，证明对于 $1\leqslant i\leqslant k$，$ia_i\leqslant n$.

证明 我们对 i 用数学归纳法.

(1)当 $i=1$ 时，由题设 $a_1\leqslant n$，所以 $i=1$ 时成立；

(2)假设结论对不大于 $i-1$ 的正整数都成立.

若对于某些整数 p 和 q，$[a_{i-1},a_i]=pa_{i-1}=qa_i$，

因为 $a_{i-1}>a_i$，则 $q>p$，

如果 $q<i$，则有 $i(q-p)\geqslant i>q,(i-1)q>ip,\frac{p}{q}<\frac{i-1}{i}$，

由归纳假设可推出 $ia_i=ia_{i-1}\frac{p}{q}<ia_{i-1}\cdot\frac{i-1}{i}=(i-1)a_{i-1}\leqslant n$，

如果 $q\geqslant i$，则由归纳假设有 $ia_i\leqslant qa_i=[a_{i-1},a_i]\leqslant n$.

于是结论对 i 成立.

由(1)、(2)，对所有 $1\leqslant i\leqslant k$，$ia_i\leqslant n$ 成立.

例 11　M_n 为 $1,2,3,\cdots,n$ 的最小公倍数（如 $M_1=1,M_2=2,M_3=6,M_4=12,M_5=60,M_6=60$），对什么样的正整数 n，$M_{n-1}=M_n$ 成立？证明你的结论.

解　若 n 是某个质数的幂，则

$n=p^k$，p 是质数.

则 $M_n=[1,2,\cdots,n-1,n]=[M_{n-1},n]=[M_{n-1},p^k]=pM_{n-1}$，

此时 $M_{n-1}\neq M_n$.

若 n 不是某个质数的幂，设

$n=ab,1<a<n,1<b<n$，则 $a\leqslant n-1,b\leqslant n-1$，

再令 $(a,b)=1$，则 $a|M_{n-1},b|M_{n-1}$.

所以 $n=ab|M_{n-1}$. 于是 $M_n=M_{n-1}$.

因此 $M_{n-1}=M_n$ 的充要条件是正整数 n 不是某个质数的幂.

能力训练

1. 设 a 和 b 是两个给定的正整数，使 $\frac{a+1}{b}+\frac{b+1}{a}$ 是一个整数，求证：a 和 b 的最大公约数不超过 $\sqrt{a+b}$.

2. 设 a,b 为正整数，且 $(a,b)=1$，证明：当整数 $n>ab-a-b$ 时，方程 $ax+by=n$ 有非负的整数解；但当 $n=ab-a-b$ 时，上述方程没有非负整数解.

3. 设 $n>1,m=2^{n-1}(2^n-1)$，证明：任一个 $k(1\leqslant k\leqslant m)$ 都可以表示为 m 的某些不同约数之和.

4. 数列 $101,104,109,116,\cdots$ 的通项是 $a_n=100+n^2$，对于每个 n，d_n 表示 a_n 与 a_{n+1} 的最大公约数，求 d_n 的最大值.

5. 设 n,k 是正整数，且 $n>k$，证明：$C_n^k,C_{n+1}^k,\cdots,C_{n+k}^k$ 的最大公约数是 1.

6. 对任给的正整数 $k(k>1)$，记 $n,n+1,\cdots,n+k$ 的最小公倍数为 $Q(n)$，$n\in\mathbf{N}_+$，证明：存在无穷多个 n，使得 $Q(n)>Q(n+1)$.

7. 100 个正整数之和为 101101，则它们的最大公约数的最大可能值为多少？证明你的结论.

8. 若 n 为小于 50 的自然数，求使代数式 $4n+5$ 和 $7n+6$ 的值有大于 1 的公约数的所有的 n 值.

9.（2005 年奥地利数学奥林匹克）确定所有的三元正整数组 (a,b,c)，使得 $a+b+c$ 是 a、b、c 的最小公倍数.

10.（2005 年加拿大数学奥林匹克）若有序三元正整数组 $\{a,b,c\}$ 满足 $a\leqslant b\leqslant c$，$(a,b,c)=1$，$a^n+b^n+c^n$ 能被 $a+b+c$ 整除，则称 $\{a,b,c\}$ 是 n-能量的. 例如，$\{1,2,3\}$ 是 5-能量的.

(1) 求出所有的有序三元正整数组，满足：对于任意 $n\geqslant 1$，其有序三元正整数组是 n-能量的；

(2) 求出所有既是 2004-能量的又是 2005-能量的但不是 2007-能量的有序三元正整数组.

§1.3 素数及算术基本定理

知识扫描

1. 素数的定义及一些基本性质　大于 1 的整数 n 至少有两个不同的正约数：1 和 n. 如果 n 没有大于 1 而小于 n 的约数，则称 n 是素数. 如果 n 有大于 1 而小于 n 的约数，即 n 可表示为 $a\cdot b$ 的形式，则称 n 为合数.

(1) 大于 1 的整数必有素因子.

(2) 既为偶数又为素数的正整数只有一个，它就是 2.

(3) 设 p 为素数，n 是任意整数，则或者 p 整除 n，或者 p 与 n 互素.

(4) 设 p 是素数，a、b 是整数，如果 $p\mid ab$，则 a、b 中至少有一个被 p 整除. 证明：如果 p 不整除 a 和 b，则 p 与 a 和 b 均互素，从而 p 与 ab 互素，矛盾！

(5) 素数有无穷多个. 用反证法证明这个命题，假设素数只有有限多个，设 $p_1=2$，$p_2=3$，…，p_k 是全部素数，考虑 $N=p_1p_2\cdots p_k+1$，显然 $N>1$. 故 N 有素因子 p. 因 p_1，p_2，…，p_k 是全部素数，故 p 必等于某个 $p_i(1\leqslant i\leqslant k)$，从而 p 整除 $N-p_1p_2\cdots p_k=1$，这不可能，因此素数有无穷多个.

2. 唯一分解定理　每个大于1的正整数均可分解成有限个素数的积.如果不计素因数在乘积中的次序,则其分解方式是唯一的,即 $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\cdots\cdot p_k^{\alpha_k}$,其中 p_i 是质数,α_i 是正整数,$1\leqslant i\leqslant k$.下面我们来证明它的唯一性,设 $n>1$ 有两种素因数分解,

$$n=p_1p_2\cdots p_k=q_1q_2\cdots q_l. \quad ①$$

我们要证明 $k=l$ 且素数 $p_1,p_2,\cdots,p_k$ 是 $q_1,q_2,\cdots,q_l$ 的一个排列.

由①可见 p_1 整除 $q_1q_2\cdots q_l$,那么 p_1 整除 q_1 或 $q_2\cdots q_l$,若 $p_1|q_1$,因 p_1,q_1 都是素数,则 $p_1=q_1$;若 $p_1|q_2\cdots q_l$,重复这一论证知,p_1 必与 $q_2,\cdots,q_l$ 之一相同,因此我们可以在①式两边约去 p_1,再考虑 p_2,并重复上述过程,最终知 n 的两种素因数分解完全相同.证毕.

3. n 的约数的标准分解　设 n 的标准分解为

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\ (p_i \text{ 是互不相等的质数},\alpha_i\in\mathbf{N}_+), \quad ②$$

则正整数 d 是 n 的约数的充分必要条件是其标准分解为

$$d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k},0\leqslant\beta_i\leqslant\alpha_i,i=1,2,\cdots,k. \quad ③$$

4. n 的正约数的个数及正约数的和　记 $r(n)$ 是 n 的正约数的个数,$\delta(n)$ 是 n 的正约数之和,且 n 的标准分解为②式,则有

$$r(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1), \quad ④$$

$$\delta(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\cdots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}. \quad ⑤$$

由于③中的指数 β_i 有 α_i+1 种选取且彼此独立,又由唯一分解定理知指数 $\beta_1,\cdots,\beta_k$ 所有可能的选取产生 k 种不同的约数,因此由乘法原理知 $r(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$,即④式.

此外,$\delta(n)$ 可表示为

$$\delta(n)=(1+p_1+\cdots+p_1^{\alpha_1})(1+p_2+\cdots+p_2^{\alpha_2})\cdots(1+p_k+\cdots+p_k^{\alpha_k}).$$

因为将上式右端的数逐项乘开后,每个形如③的数恰恰出现一次,即给出了所有正约数,即 $\delta(n)=\frac{p^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p^{\alpha_2+1}-1}{p_2-1}\cdot\cdots\cdot\frac{p^{\alpha_k+1}-1}{p_k-1}$.

5. n 为平方数的充要条件　n 为平方数的充要条件是 $r(n)$ 为奇数.

由于 $r(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$,则 $r(n)$ 为奇数等价于 $\alpha_1+1,\alpha_2+1,\cdots,\alpha_n+1$ 都是奇数,等价于 $\alpha_1,\alpha_2,\cdots,\alpha_k$ 都是偶数,由 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 得,等价于 n 为完全平方数.

6. 素数的一个判别法　设 $n>1$,且 n 不被不超过 $\sqrt{n}$ 的素数整除,则 n 是素数.

证明:若 n 不是素数,则 $n=ab$,a,b 都大于1,无妨设 $a\geqslant b$,则 $b\leqslant\sqrt{n}$,因为 $b>1$,故 b 有素因子 p,又 $b|n$,从而 $p|n$,但 $p\leqslant b\leqslant\sqrt{n}$,矛盾!

7. $n!$ 的标准分解　对任意正整数 m 及素数 p,记号 $p^{\alpha}\parallel m$ 表示 $p^{\alpha}|m$ 但 $p^{\alpha+1}\nmid m$,即

p^{α} 是 m 的标准分解中出现的 p 的幂，$\alpha=\sum_{i=1}^{\infty}\left[\frac{m}{p^{i}}\right]$.

由于当 $p^{i}>m$ 时，$\left[\frac{m}{p^{i}}\right]=0$，故上式中的和只有有限多个项不为零.

例题分析

例 1 （2003 年德国数学竞赛）证明：对任意六个连续正整数，存在一个质数，使得这个质数能且只能整除六个数之一.

证明 记这六个数为 $n,n+1,\cdots,n+5$.

若 n 不能被 5 整除，则 $n+1$ 至 $n+4$ 中确只有一个数能被 5 整除.

若 n 能被 5 整除，则 $n+1$ 至 $n+4$ 中有两个整数不能被 2、5 整除，其中至少有一个不能被 3 整除.

因此，该数至少有一个大于 5 的质因子，且该质数不能整除另外五个整数.

例 2 求所有这样的素数，它既是两素数之和，同时又是两素数之差.

分析 考虑素数 2 是素数中唯一的偶数.

解 设所求的素数是 p，因它是两素数之和，故 $p>2$.

从而 p 是奇数，因此和为 p 的两个素数中有一个为 2.

同时差为 p 的两素数中，减数也是 2，即 $p=q+2$，$p=r-2$，其中 q,r 是素数.

于是 $p-2,p,p+2$ 均为素数.

而 $p-2,p,p+2$ 是三个连续的奇数，必定有一个是 3 的倍数.

因为这个数是素数，故只能是 3.

经检验，只有 $p-2=3,p=5,p+2=7$ 时，才满足条件，故 $p=5$.

例 3 （第 29 届俄罗斯数学奥林匹克）证明：从任意 5 个互质的三位数中，能选出 4 个数是互质的.

分析 先将任意 4 个数的最大公约数设出来，再利用反证法证明这 5 个公约数中至少有 1 个为 1.

证明 设这 5 个数为 a_1、a_2、a_3、a_4、a_5.

若题设不成立，则存在

$(a_1,a_2,a_3,a_5)=d_1,(a_1,a_2,a_3,a_4)=d_2,(a_1,a_3,a_4,a_5)=d_3,$

$(a_1,a_2,a_4,a_5)=d_4,(a_2,a_3,a_4,a_5)=d_5.$

其中，d_1,d_2,d_3,d_4,d_5 两两互质，且均不为 1，不妨设 $d_1>d_2>d_3>d_4>d_5$，则

$a_1=b_1d_1d_2d_3d_4\geqslant b_1\times3\times5\times7\times11=1155b_1\geqslant1155>1000.$

矛盾！

因此，d_1、d_2、d_3、d_4、d_5 中必有一个为 1.

即从任意 5 个互质的三位数中，能找出 4 个互质.

例 4 （第 15 届亚太地区数学奥林匹克）设整数 k，$k\geqslant 14$，p_k 是小于 k 的最大质数，若 $p_k\geqslant\frac{3k}{4}$，n 是一个合数，证明：

(1)若 $n=2p_k$，则 n 不能整除 $(n-k)!$.

(2)若 $n>2p_k$，则 n 能整除 $(n-k)!$.

证明 (1)$n=2p_k$ 时，

因为 $k>p_k$，则 $p_k>2p_k-k=n-k$，所以，$p_k\nmid(n-k)!$，故 $n\nmid(n-k)!$.

(2)$n>2p_k$ 时，

因为 n 是合数，故设 $n=ab(2\leqslant a\leqslant b)$，若 $a\geqslant 3$.

(ⅰ)$a\neq b$，则 $n>2p_k\geqslant\frac{3k}{2}$，$b\leqslant\frac{n}{3}$.

从而，$k<\frac{2n}{3}$，故 $n-k>\frac{n}{3}\geqslant b>a$.

所以 $n\mid(n-k)!$.

(ⅱ)$a=b$，则 $n=a^2$，$n-k>\frac{n}{3}=\frac{a^2}{3}$，

因为 $k\geqslant 14$，则 $p_k\geqslant 13$，$n\geqslant 26$，$a\geqslant 6$，

从而$\frac{a^2}{3}\geqslant 2a$. 故 $n-k>2a$. 所以，$n\mid(n-k)!$.

若 $a=2$，因为 $n\geqslant 26$，假设 b 不为质数，则 $b=b_1b_2(b_1\leqslant b_2)$，

因为 $b\geqslant 13$，则 $b_2\geqslant 4$，于是 $ab_1\geqslant 4$ 归入 $a\geqslant 3$ 的情况，

不妨设 b 为质数，则 $b=\frac{n}{2}>p_k$，

因为 p_k 是小于 k 的最大质数，则 $b>k$，

从而 $n-k=2b-k>b$. 所以，$n\mid(n-k)!$.

综上所述，$n>2p_k$ 时，$n\mid(n-k)!$.

例 5 （2002 年澳大利亚国家数学竞赛）求所有质数 p、q、r，使得 p^q+p^r 为完全平方数.

分析 分 $q=r$ 和 $q\neq r$ 这两种情况讨论，而 $q\neq r$ 时不妨设 $q<r$，并将 p^q+p^r 变成 $p^q(1+p^{r-q})$. 由完全平方数的性质及$(p^q,1+p^{r-q})=1$，得 p^q，$1+p^{r-q}$ 均为完全平方数，从而使问题得到了简化.

解 若 $q=r$，则 $p^q+p^r=2p^q$.

所以 $p=2$，q 为奇质数.

故$(2,q,q)$为满足条件的三元质数组，其中质数$q\geqslant 3$.

若$q\neq r$，不失一般性，设$q<r$，则$p^q+p^r=p^q(1+p^s)$，其中$s=r-q\geqslant 1$.

由于p^q和$1+p^s$的最大公因数为1，

所以p^q和$1+p^s$均为完全平方数. 故$q=2$.

由于$1+p^s$为完全平方数，

设$1+p^s=u^2$，即$p^s=u^2-1=(u+1)(u-1)$.

因为$u+1$与$u-1$的最大公因数为1或2，

所以当最大公因数为2时，u为奇数，p为偶数，即$p=2$，且$u-1$和$u+1$均为2的幂，于是u为3，从而$1+2^s=3^2$.

所以$s=3$，$r=q+s=2+3=5$.

故满足条件的三元质数组为$(2,2,5)$和$(2,5,2)$.

当$u+1$和$u-1$的最大公因数为1时，u为偶数，$u-1$必须为1，否则$u-1$和$u+1$可表示为不同奇质数的乘积，所以，不可能是一个质数的整数次幂，于是

$u=2$，$p^s=(u-1)(u+1)=3$，$p=3$，$s=1$，$r=q+s=3$.

故满足条件的三元质数组为$(3,2,3)$和$(3,3,2)$.

综上所述，原命题的解为$(2,2,5)$，$(2,5,2)$，$(3,2,3)$，$(3,3,2)$，$(2,q,q)$，其中质数$q\geqslant 3$.

例6 求三个素数，使得它们的积为和的5倍.

分析 将三个素数用p,q,r表示出来，利用质数性质易解出p,q,r.

解 设三个素数为p,q,r，

则$pqr=5(p+q+r)$，

于是p,q,r中必有一个等于5. 不妨设$r=5$，

则$5pq=5(p+q+5)$，

即$pq=p+q+5$，$(p-1)(q-1)=6$.

由$p>1$，$q>1$可知

$\begin{cases}p-1=2\\q-1=3\end{cases}$或$\begin{cases}p-1=3\\q-1=2\end{cases}$或$\begin{cases}p-1=1\\q-1=6\end{cases}$或$\begin{cases}p-1=6\\q-1=1\end{cases}$

由于$p=4$或$q=4$不是素数，

所以只有$p=2$，$q=7$或$p=7$，$q=2$.

于是所求素数为2，5，7.

例7 数20！有多少个正整数因数？

分析 将20！写成其标准分解式$n=\beta_1^{\alpha_1}\beta_2^{\alpha_2}\cdots\beta_k^{\alpha_k}$，再利用$r(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$可计算出结果.

解 由于小于 20 的素数为 2,3,5,7,11,13,17,19,在 20! 的标准分解式中,

2 的最高指数 $=\left[\frac{20}{2}\right]+\left[\frac{20}{4}\right]+\left[\frac{20}{8}\right]+\left[\frac{20}{16}\right]=18$,

3 的最高指数 $=\left[\frac{20}{3}\right]+\left[\frac{20}{9}\right]=8$,

5 的最高指数 $=\left[\frac{20}{5}\right]=4$,

7,11,13,17,19 的最高指数分别为 2,1,1,1,1.

于是 20! 的标准分解式为

$20!=2^{18}\cdot 3^{8}\cdot 5^{4}\cdot 7^{2}\cdot 11\cdot 13\cdot 17\cdot 19$

于是 20! 中正约数 $r(20!)$ 个数为:

$$\begin{aligned}r(20!)&=(18+1)(8+1)(4+1)(2+1)(1+1)(1+1)(1+1)(1+1)\\&=19\cdot 9\cdot 5\cdot 3\cdot 2\cdot 2\cdot 2\cdot 2\\&=41040.\end{aligned}$$

所以 20! 的正约数的个数为 41040 个.

例 8 求自然数 N,使它能被 5 和 49 整除,并且包括 1 和 N 在内,它共有 10 个约数.

解 把 N 写成素因数分解形式

$N=2^{a_1}\cdot 3^{a_2}\cdot 5^{a_3}\cdot 7^{a_4}\cdots p_n^{a_n}$,其中 $a_i\geqslant 0, i=1,2,\cdots,n$,

则它所有约数的个数为

$(a_1+1)(a_2+1)(a_3+1)(a_4+1)\cdots(a_n+1)=10$.

由于 $5\mid N, 7^2\mid N$,则 $a_3+1\geqslant 2, a_4+1\geqslant 3$,

因此 $a_1,a_2,a_5,a_6,\cdots,a_n$ 必然都为 0.

即 $N=5^{a_3}\cdot 7^{a_4}$.

由于 $(a_3+1)(a_4+1)=10=2\times 5$,可得 $a_3=1, a_4=4$,

即本题有唯一解 $N=5\cdot 7^4$.

例 9 如果 p,q 是两个素数,并且 $q=p+2$,证明:p^q+q^p 能被 $p+q$ 整除.

分析 由题设 $q=p+2$,对 p^q+q^p 进行变形,有 $p^q+q^p=(p^p+q^p)+(p^{p+2}-p^p)$,则需证明 $p+q\mid p^{p+2}-p^p$. 而 $p+q=2(p+1)$,只需证明 $2(p+1)\mid p^{p+2}-p^p$.

证明
$$\begin{aligned}p^q+q^p&=(p^p+q^p)+(p^q-p^p)\\&=(p^p+q^p)+(p^{p+2}-p^p),\end{aligned}$$

因为 p、q 都为素数,且 $q=p+2$,则 p,q 都是奇数,则 $p+q\mid p^p+q^p$.

又 $p^{p+2}-p^p=p^p(p+1)(p-1)$,

由于 $p-1$ 为偶数,则 $2(p+1)\mid p^p(p+1)(p-1)$.

又 $2(p+1)=2p+2=p+q$,

于是 $p+q\mid p^{p+2}-p^p$，因此 $p+q\mid p^q+q^p$.

能力训练

1. 证明：正整数 n 的正约数的个数不超过 $2\sqrt{n}$.

2. 求最小的正整数 n，满足：(1) n 恰有 144 个不同的正因数；(2) 在 n 的正因数中有 10 个连续整数.

3. 已知方程 $x^4-px^3+q=0$ 有一整数根，求素数 p、q.

4. 试求出所有不超过 1000 的素数 p，这些 p 使 $2p+1$ 是自然数的方幂（亦即存在自然数 m、n，$n\geqslant 2$，使 $2p+1=m^n$）.

5. 证明：从任意 6 个互质的四位数中能选出 5 个数是互质的.

6. 设 n 是满足下列条件的正整数中最小的数.(1) n 是 75 的倍数；(2) n 恰有 75 个正整数因子（包括 1 及本身），试求 $\frac{n}{75}$.

7.（2003 年 IMO 斯洛文尼亚国家队选拔赛）设 S 是大于 1 的正整数有限非空集合，并具有以下性质：存在一个数 $s\in S$，满足：对任何正整数 n，或者 $(s,n)=1$，或者 $(s,n)=s$. 证明：一定存在两个数 s、$t\in S$（s，t 不一定相异），使得 (s,t) 是质数.

8. 设 $p_1,p_2,\cdots,p_{24}$ 是一些不小于 5 的素数，证明：$p_1^2+p_2^2+\cdots+p_{24}^2$ 可被 24 整除.

9.（2005 年罗马尼亚数学奥林匹克）证明：对每一个正整数 n，在十进制表示下，存在唯一的 n 位正整数能被 5^n 整除，其每一位数字都属于数集 $\{1,2,3,4,5\}$.

10.（2005 年美国数学奥林匹克）求所有正整数 n，满足 n 为合数，且其所有大于 1 的因数可以放在一个圆上，使得任意两个相邻的因数都不是互质的.

第二章 同 余

§2.1 同余的概念和定义

知识扫描

(一)**定义1** 设 m 是一个给定的正整数，如果两个整数 a，b 用 m 除所得的余数相同，则称 a，b 对模 m 同余，记为：$a\equiv b(\bmod m)$. 否则记为 $a\not\equiv b(\bmod m)$.

例如：$18\equiv 2(\bmod 8)$ $59\not\equiv 3(\bmod 9)$.

(二)同余的基本性质

(1)$a\equiv 0(\bmod m)\Leftrightarrow m\mid a$；

(2)若 $a\equiv b(\bmod m)$，$b\equiv c(\bmod m)$，则 $a\equiv c(\bmod m)$；

(3)若 $a\equiv b(\bmod m)$，$c\equiv d(\bmod m)$，则 $a\pm c\equiv b\pm d(\bmod m)$，$ac\equiv bd(\bmod m)$；

(4)若 $ac\equiv bc(\bmod m)$，$c\neq 0$，则 $a\equiv b\left(\bmod \dfrac{m}{(m,c)}\right)$，特别地，若 $(m,c)=1$，则 $a\equiv b(\bmod m)$；

(5)若 $a\equiv b(\bmod m)$ 而 $d\mid m$，$(d>0)$，则 $a\equiv b(\bmod d)$；

(6)若 $a\equiv b(\bmod m)$，$c>0$，则 $ac\equiv bc(\bmod m)$；

(7)若 $a\equiv b(\bmod m_1)$，$a\equiv b(\bmod m_2)$，则 $a\equiv b(\bmod [m_1,m_2])$，特别地，若 $(m_1,m_2)=1$，则 $a\equiv b(\bmod m_1m_2)$；

(8)若 $a\equiv b(\bmod m)$，则 $(a,m)=(b,m)$；

(9)若 $a_i\equiv b_i\pmod{m}$，$i=0,1,2,\cdots,n$，则 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0\pmod{m}$. 特别地，设 $f(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0$（$c_i\in\mathbf{Z}$），若 $a\equiv b\pmod{m}$，则 $f(a)\equiv f(b)\pmod{m}$.

例题分析

例 1 （2001 年爱尔兰数学奥林匹克）求最小正整数 a，使得存在正奇数 n 满足 $2001\mid 55^n+a\cdot 32^n$.

分析 运用同余性质，注意到 $2001=23\times 87$，我们可求得 $a\equiv 1\pmod{87}$ 和 $a\equiv -1\pmod{23}$. 于是便可得到满足要求的 a 的最小值.

解 由于 $2001=87\times 23$. 由题意知，存在正奇数 n，使得

$87\mid 55^n+a\cdot 32^n$， ①

且 $23\mid 55^n+a\cdot 32^n$. ②

由①知：$0\equiv 55^n+a\cdot 32^n\pmod{87}$

$\equiv(-32)^n+a\cdot 32^n\pmod{87}$

$\equiv 32^n(a-1)\pmod{87}$.

又 $(32^n,87)=1$，故 $a-1\equiv 0\pmod{87}$ ③

由②知：$0\equiv 55^n+a\cdot 32^n\pmod{23}$

$\equiv 32^n+a\cdot 32^n\pmod{23}$.

又 $(32^n,23)=1$，所以 $a+1\equiv 0\pmod{23}$，

故 $a\equiv -1\pmod{23}$ ④

由③设 $a=87k+1$（$k\in\mathbf{N}$）代入④得

$23\mid 87k+2\Rightarrow 23\mid 18k+2\Rightarrow 23\mid -5k+25\Rightarrow 23\mid k-5$

又 $k\geqslant 0$，所以 $k\geqslant 5$.

于是 a 的最小值为 $87\times 5+1=436$.

点评 当模不为质数时，一般情况下将模分解为质数进行考虑.

例 2 设 p 是一个素数，$1\leqslant k\leqslant p-1$，试证：$C_{p-1}^k\equiv(-1)^k\pmod{p}$.

证明 设 $C_{p-1}^k\equiv A\pmod{p}$，则：

$$A\equiv\frac{(p-1)(p-2)\cdots(p-k)}{k!}\pmod{p},$$

所以 $k!\cdot A\equiv(p-1)(p-2)\cdots(p-k)\pmod{p}$，

$\equiv(-1)\cdot(-2)\cdots(-k) \pmod p$

$\equiv(-1)^k k! \pmod p$.

又$(k!,p)=1$，

所以$A\equiv(-1)^k \pmod p$，

所以$C_{p-1}^k\equiv(-1)^k \pmod p$.

点评 用类似的方法我们还可以证明以下几个非常有用的结论：

①若p为奇质数，则$C_p^k\equiv 0 \pmod p\ (1\leqslant k\leqslant p-1)$；

②若p为奇质数，则对于$m\in\mathbf{N}_+$，有

$C_m^p\equiv\left[\frac{m}{p}\right] \pmod p$.

例 3 已知$p-2$与p均为质数，$k=\left[\frac{2p-1}{3}\right]$. 试证：$S=1+\frac{C_{p-1}^1}{2}+\frac{C_{p-1}^2}{3}+\cdots+\frac{C_{p-1}^{k-1}}{k}$为整数且为$p$的倍数.

证明 (1)当$p\geqslant 7$时，易知$p\equiv 1 \pmod 6$，设$p=6m+1$，

则$k=\left[\frac{2p-1}{3}\right]=4m$.

又对于$1\leqslant l\leqslant k$.

$\frac{C_{p-1}^{k-1}}{k}=\frac{(p-1)!}{k(k-1)!\ (p-k)!}=\frac{(p-1)!}{k!\ (p-k)!}=\frac{p!}{p\cdot k!\ (p-k)!}=\frac{1}{p}\cdot C_p^k$.

所以$S=1+\frac{C_{p-1}^1}{2}+\cdots+\frac{C_{p-1}^{k-1}}{k}=\frac{1}{p}\sum\limits_{k_0=1}^{k}C_p^{k_0}$.

又对于$1\leqslant k_0\leqslant k$，$C_p^{k_0}=\frac{p!}{k_0!\ (p-k_0)!}=\frac{p}{k_0}C_{p-1}^{k_0-1}$，所以$p\mid k_0C_p^{k_0}$，

又$(p,k_0)=1$，所以$p\mid C_p^{k_0}$.

所以S为整数.

下面证明：S为p的倍数.

$C_p^{k_0}=p\frac{(p-1)(p-2)\cdots(p-k_0+1)}{k_0!}=p\frac{p\cdot f(k_0)+(-1)^{k_0-1}(k_0-1)!}{k_0!}$，

其中$f(k_0)$为整数.

$$\begin{aligned}\text{所以 } S&=p\sum_{k_0=1}^{k}\frac{f(k_0)}{k_0!}+\sum_{k_0=1}^{k}\frac{(-1)^{k_0-1}(k_0-1)!}{k_0!}\\&=p\sum_{k_0=1}^{k}\frac{f(k_0)}{k_0!}+\sum_{k_0=1}^{k}(-1)^{k_0-1}\frac{1}{k_0}\\&=p\sum_{k_0=1}^{k}\frac{f(k_0)}{k_0!}+1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+(-1)^{k-1}\frac{1}{k}\end{aligned}$$

$$=p\frac{A}{k!}+\sum_{k_0=1}^{k}(-1)^{k_0-1}\frac{1}{k_0},$$

其中 A 为整数.

又 $\sum\limits_{k_0=1}^{k}\frac{(-1)^{k_0-1}}{k_0}=1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{4m-1}-\frac{1}{4m}$

$$=\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{4m}\right)-2\left(\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{4m}\right)$$

$$=\frac{1}{2m+1}+\frac{1}{2m+2}+\cdots+\frac{1}{4m}$$

$$=\frac{6m+1}{(2m+1)\cdot 4m}+\frac{6m+1}{(2m+2)(4m-1)}+\cdots+\frac{6m+1}{3m\cdot(3m+1)}$$

$$=p\cdot\frac{B}{k!}.$$

其中 B 为整数.

所以 $S=p\frac{A}{k!}+\frac{B}{k!}p=p\frac{A+B}{k!}$.

又 S 为整数,所以 $k!\mid p(A+B)$.

因为 $(p,k!)=1$,所以 $k!\mid A+B$. 所以 $p\mid S$.

所以 S 为 p 的倍数.

(2)当 $p\leqslant 6$,则易知 $p=5$,$k=\left[\frac{2p-1}{3}\right]=3$.

所以 $S=1+\frac{C_4^1}{2}+\frac{C_4^2}{3}=1+2+2=5$.

所以 S 为整数且为 p 的倍数.

综上所述原命题得证.

例 4 (2004 年 IMO 预选题)设 $p_1,p_2,\cdots,p_n$ 是大于 3 的 n 个互异的素数,试证:$2^{p_1\cdot p_2\cdot\cdots\cdot p_n}+1$ 至少有 4^n 个因数.

证明 若奇数 u,v 满足 $(u,v)=1$,则 2^u+1 和 2^v+1 均可以被 3 整除. 设 $(2^u+1,2^v+1)=t$,若 $t>3$,则 $2^u\equiv-1(\bmod t)$,$2^v\equiv-1(\bmod t)$.

又 u,v 均为奇数,

所以 $(-2)^u\equiv1(\bmod t)$,$(-2)^v\equiv1(\bmod t)$.

考虑同余方程 $(-2)^x\equiv1(\bmod t)$,

由于 u,v 是该同余方程的解,所以一定存在最小正整数 r 是该方程的解,

即 $(-2)^r\equiv1(\bmod t)$,显然 $r>2$.

若该方程的解为 $x=rp+q$,$0<q<r$,则

$(-1)^x\equiv(-1)^{rp+q}\equiv[(-1)^r]^p\cdot(-1)^q\equiv(-1)^q(\bmod t)$,

于是 q 也是该方程的解，与 r 的最小性矛盾！

所以 $q=0$.

由上知：$r|u,r|v$，所以 $r|(u,v)$.

又 $(u,v)=1$，

所以 $r|1\Rightarrow r=1$，矛盾！

所以 $(2^u+1,2^v+1)=3$.

因为 $2^{uv}+1=(2^u)^v+1$

$$=(2^u+1)((2^u)^{v-1}-(2^u)^{v-2}+\cdots+(2^u)^2-2^u+1),$$

所以 $2^u+1|2^{uv}+1$. ①

同理 $2^v+1|2^{uv}+1$. ②

由①、②得 $[2^u+1,2^v+1]|2^{uv}+1$，

所以 $\dfrac{(2^u+1)(2^v+1)}{3}\Big|2^{uv}+1$.

下面用数学归纳法证明原命题：

(1)当 $n=1$ 时，$2^{p_1}+1$ 至少有 4 个因数，即 $1,3,\dfrac{2^{p_1}+1}{3},2^{p_1+1}$，(由于 $p_1\geqslant 5$，则 $\dfrac{2^{p_1}+1}{3}\neq 3$)；

(2)假设 $2^{p_1p_2\cdots p_{n-1}}+1$ 至少有 4^{n-1} 个因数，对于 $2^{p_1p_2\cdots p_n}+1$，

设 $u=p_1p_2\cdots p_{n-1}$，$v=p_n$. 由于 $(2^u+1,\dfrac{2^v+1}{3})=1$，

所以 $m=\dfrac{1}{3}(2^u+1)(2^v+1)$ 至少有 $2\cdot 4^{n-1}$ 个因数.

因为 $m|2^{uv}+1$，

又 $u,v\geqslant 5$，所以 $uv\geqslant 2(u+v)$，

所以 $2^{uv}+1\geqslant 2^{2(u+v)}+1>m^2$.

于是 $2^{uv}+1$ 的因数个数不小于 m 的因数个数的 2 倍.(因为若 $q|m$，则 $q|2^{uv}+1\Rightarrow \dfrac{2^{uv}+1}{q}|2^{uv}+1$)

所以 $2^{uv}+1$ 的因数个数不少于 4^n.

故结论得证.

点评 本题解答中前半部分证明了一个有用的结论：若奇数 u,v 满足 $(u,v)=1$，$u,v\in\mathbf{N}_+$，则 $(2^u+1,2^v+1)=3$.

能力训练

一、选择题

1. 已知 A 是十进制表示为 4568^{7777} 的各位数字之和，B 是 A 的各位数字之和，C 是 B 的各位数字之和，则 $C=$（　　）

A. 5　　B. 32　　C. 9　　D. 14

2. 数 104^{2006} 被 29 除的余数为（　　）

A. 5　　B. 27　　C. 28　　D. 13

3. 2006！的末尾零的个数为（　　）

A. 499　　B. 500　　C. 501　　D. 502

4. $1\times3\times5\times7\times\cdots\times1997\times1999\times2001\times2003\times2005$ 的末三位数为（　　）

A. 125　　B. 375　　C. 625　　D. 875

5. 使 $p+10$，$p+14$ 都是素数的素数 p（　　）

A. 不存在　　B. 有 1 个

C. 有无穷多个　　D. 不只一个，但只有有限个

6. 若质数 $p\equiv3(\bmod 4)$，且 $a^2+b^2\equiv0(\bmod p)$，则（　　）

A. $p|a$，$p|b$　　B. $p\nmid a$，$p\nmid b$　　C. $p|a$ 且 $p\nmid b$　　D. $p\nmid a$，$p|b$

二、填空题

7. p 是大于 5 的质数，p^2 除以 30 的余数为________.

8. 数 1059，1417，2312 被 d 除的余数相同，$d>1$，则整数 $d=$________.

9. $3333^{8888}+8888^{3333}\equiv$________$(\bmod 7)$.

10. 若 p 为奇质数，则 $\left(a+b,\dfrac{a^p+b^p}{a+b}\right)=$________.（其中 $(a,b)=1$）

11. 使得不存在非负整数 a，b 满足 $|3^a-2^b|=p$ 的最小素数 $p(p>3)$ 为________.

12. 数列 $\{a_n\}$ 定义如下：$a_0=1$，$a_1=2$，$a_{n+2}=a_n+a_{n+1}^2$，则 $a_{2006}\equiv$________$(\bmod 7)$.

三、解答题

13. 设集合 $\{1,2,3,\cdots,1998\}$ 被分为 999 个彼此不交的二元子集 $\{a_i,b_i\}$，并且对 $1\leqslant i\leqslant999$，均有 $|a_i-b_i|=1$ 或 6，试证：和数 $\sum\limits_{i=1}^{999}|a_i-b_i|$ 的末位数字为 9.

14. 设 a 为奇数，n 为正整数，试证：$a^{2^n}\equiv1(\bmod 2^{n+2})$.

15. 对于自然数 n，只要 $n|a^n-1$，就有 $n^2|a^n-1$，则称 n 具有性质 p. 试证：

(1) 每个质数 n 都具有性质 p；

(2) 存在无穷多个非素数 n 具有性质 p.

§2.2 完系、简系、剩余类

知识扫描

若按对某一模 m 的余数进行分类，就可以引入所谓的剩余类和完全剩余系的概念.

定义 2 设 $m\in\mathbf{N}_+$，把全体整数按其对模 m 的余数 $r(0\leqslant r\leqslant m-1)$ 归为一类，记为 k_r，每一类 $k_r(r=0,1,2,\cdots,m-1)$ 均称为模 m 的剩余类(又叫同余类)，同一类中任一数称为该类中另一数的剩余.

根据定义，剩余类具有如下性质：

(1)$\mathbf{Z}=k_0\cup k_1\cup k_2\cup\cdots\cup k_{m-1}$，而 $k_i\cap k_j=\varnothing(i\neq j)$；

(2)对于 $\forall n\in\mathbf{Z}$，有唯一的 $r_0\in\{0,1,2,\cdots,m-1\}$，使得 $n\in k_{r_0}$；

(3)对 $\forall a,b\in\mathbf{Z}$，$a,b\in k_r\Leftrightarrow a\equiv b(\bmod m)$.

定义 3 设 $k_0,k_1,\cdots,k_{m-1}$ 是模 m 的全部剩余类，从每个 k_r 中任取一个数 a_r，这 m 个数 $a_0,a_1,a_2,\cdots,a_{m-1}$ 组成的一个组称为模 m 的一个完全剩余系，简称完系.

显然，模 m 的完全剩余系有无穷多个，但最常用的是下面两个：

(1)最小非负剩余系：$0,1,2,\cdots,m-1$；

(2)最小绝对值剩余系：它随 m 的奇偶性不同而略有区别.

当 $m=2k+1$ 时，为 $-k,-k+1,\cdots,-1,0,1,2,\cdots,k-1,k$.

当 $m=2k$ 时，为 $-(k-1),-(k-2),\cdots,-1,0,1,2,\cdots,k$，或 $-k,-(k-1),\cdots,-1,0,1,2,\cdots,k-2,k-1$.

关于完全剩余系，有以下判别方法：

(1)m 个整数 $a_1,a_2,a_3,\cdots,a_{m-1},a_m$ 是模 m 的一个完系 $\Leftrightarrow$ 当 $1\leqslant i<j\leqslant m$ 时，$a_i\not\equiv a_j(\bmod m)$；

(2)设 $(b,m)=1$，c 为任意整数，若 $a_1,a_2,a_3,\cdots,a_m$ 是模 m 的一个完系，则 $ba_1+c,ba_2+c,ba_3+c,\cdots,ba_m+c$ 也是模 m 的一个完系.

特别地，任意 m 个连续的整数构成模 m 的一个剩余系.

设 m 为一正整数，由于在 $0,1,2,\cdots,m-1$ 中与 m 互质的数的个数是由 m 唯一确定的一个正整数，因此可以给出以下定义：

定义 4 m 为一正整数，把 $0,1,2,\cdots,m-1$ 中与 m 互质的数的个数叫做 m 的欧拉函

数，记为$\varphi(m)$.

设k是模m的一个剩余类，若$a,b\in k$，则$a\equiv b(\bmod m)$，于是$(a,m)=(b,m)$. 因此若$(a,m)=1$，则k中的任一数均与m互质. 这样，又给出如下定义：

定义 5 如果一个模m的剩余类k_r中任一数与m互质，则称k_r是与模m互质的剩余类，在与模m互质的每个剩余类中任取一个数（共$\varphi(m)$个）所组成的数组，称为模m的一个简化剩余系（简称为简系）.

由此定义，不难得到如下关于模m简化剩余系的判定方法：

(1)$a_1,a_2,a_3,\cdots,a_{\varphi(m)}$是模$m$的简化剩余系$\Leftrightarrow(a_i,m)=1$且对于$\forall 1\leqslant i<j\leqslant m$，$a_i\not\equiv a_j(\bmod m)$；

(2)在模m的一个完全剩余系中，取出所有与m互质的数组成的数组，就是一个模m的简化剩余系；

(3)设$a_1,a_2,\cdots,a_{\varphi(m)}$是模$m$的简化剩余系，若$(k,m)=1$，则$ka_1,ka_2,ka_3,\cdots,ka_{\varphi(m)}$也是模$m$的简化剩余系.

由欧拉函数$\varphi(m)$的定义，我们用容斥原理不难给出$\varphi(m)$的计算公式：

设m的标准分解式为$m=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\cdots\cdot p_k^{\alpha_k}$，

则$\varphi(m)=m\cdot\prod\limits_{i=1}^{k}\left(1-\dfrac{1}{p_i}\right)$.

读者应认识到，引入剩余类的概念事实上为我们研究全体整数提供了一个很好的渠道.

例题分析

例 1 设n为偶数，$a_1,a_2,\cdots,a_n$与$b_1,b_2,\cdots,b_n$均是模n的完全剩余系. 试证：$a_1+b_1,a_2+b_2,\cdots,a_n+b_n$不是模$n$的完全剩余系.

分析 本题给人的第一感觉便是用反证法.

证明 如果有一组$a_i(1\leqslant i\leqslant n)$及$b_i(1\leqslant i\leqslant n)$使$a_1+b_1,a_2+b_2,\cdots,a_n+b_n$是模$n$的完全剩余系，则

$$\begin{aligned}1+2+\cdots+n&\equiv\sum_{k=1}^{n}(a_k+b_k)\pmod n\\&\equiv\sum_{k=1}^{n}a_k+\sum_{k=1}^{n}b_k\pmod n\\&\equiv2\cdot(1+2+\cdots+n)\pmod n\end{aligned}$$

及$\dfrac{n(n+1)}{2}\equiv n(n+1)\pmod n$

所以 $n\mid\frac{n(n+1)}{2}$，所以 $2n\mid n(n+1)\Rightarrow 2\mid n+1$，这与 n 为偶数矛盾！

所以原命题得证.

例 2 （2003 年克罗地亚数学奥林匹克）对于所有奇质数和正整数 $n(n\geqslant p)$，试证：$C_n^p\equiv\left[\frac{n}{p}\right](\bmod p)$.

分析与解 注意到 $C_n^p=\frac{n(n-1)\cdots(n-p+1)}{p!}$，而 $n,n-1,\cdots,n-p+1$ 组成模 p 的一个完系，于是存在 $a\in\{n,n-1,\cdots,n-p+1\}$ 使得 $p\mid a$，显然 $a=p\cdot\left[\frac{n}{p}\right]$. 设 $C_n^p\equiv c(\bmod p)$.

则 $C_n^p=\frac{n(n-1)\cdots(a+1)(a-1)(a-2)\cdots(n-p+1)\cdot a}{(p-1)!\ p}(\bmod p)$

$$=\frac{n(n-1)\cdots(a+1)(a-1)(a-2)\cdots(n-p+1)\cdot\left[\frac{n}{p}\right]}{(p-1)!}(\bmod p).$$

所以 $p\mid c\cdot(p-1)!\ -\left[\frac{n}{p}\right]n(n-1)\cdots(a+1)(a-1)\cdots(n-p+1)$.

注意到 $n(n-1)\cdots(a+1)(a-1)(a-2)\cdots(n-p+1)\equiv(p-1)!\ (\bmod p)$，

所以 $p\mid\left(c-\left[\frac{n}{p}\right]\right)\cdot(p-1)!$.

又 $(p,(p-1)!)=1$，所以 $p\mid c-\left[\frac{n}{p}\right]$. 所以 $c\equiv\left[\frac{n}{p}\right](\bmod p)$.

即 $C_n^p\equiv\left[\frac{n}{p}\right](\bmod p)$.

点评 完系在题目中一般是比较隐蔽的，发现并利用它是很重要的.

例 3 设 n 为正整数，整数 k 与 n 互质，且 $0<k<n$. 令 $M=\{1,2,\cdots,n-1\}$，给 M 中每个数染上黑白两种染色中的一种，染法如下：（ⅰ）对 M 中每个 i，i 与 $n-i$ 同色，（ⅱ）对 M 中每个 i，$i\neq k$，i 与 $|k-i|$ 同色，试证：M 中所有的数必为同色.

分析 由 $(k,n)=1$ 可以对 M 中的数重新排序，然后只需证相邻两数同色即可.

证明 因为 $(k,n)=1$，$0,1,2,\cdots,n-1$ 是模 n 的一个完系，

所以 $k\cdot0,k\cdot1,k\cdot2,\cdots,k(n-1)$ 也是模 n 的一个完系.

若设 $r_j\equiv jk(\bmod n)$（其中 $1\leqslant r_j\leqslant n-1$，$j=1,2,\cdots,n-1$），

则 $M=\{1,2,3,\cdots,n-1\}=\{r_1,r_2,\cdots,r_{n-1}\}$，

下面只需证：

r_j 与 r_{j+1} 同色 $(1\leqslant j\leqslant n-2)$. ①

显然 $r_{j+1}\equiv(j+1)k(\mathrm{mod}\,n)\equiv r_j+k(\mathrm{mod}\,n)$.

下面分两种情况讨论：

(1)若 $r_j+k<n$，则 $r_{j+1}=r_j+k$，于是由条件(ⅱ)知，r_{j+1} 与 $|r_{j+1}-k|=r_j$ 同色；

(2)若 $r_j+k>n$，则 $r_{j+1}=r_j+k-n$，于是由条件(ⅰ)知，$k-r_{j+1}=n-r_j$ 与 $n-(n-r_j)=r_j$ 同色，又由条件(ⅱ)知 $k-r_{j+1}$ 与 $|k-r_{j+1}-k|=r_{j+1}$ 同色，于是 r_{j+1} 与 r_j 同色.

所以①得证.

综上知，原命题得证.

例 4 (2001 年第 42 届 IMO 试题)设 n 为奇数且大于 1，$k_1,k_2,\cdots,k_n$ 为给定的整数，对于 $1,2,\cdots,n$ 的 $n!$ 个排列中的每一个排列 $a=(a_1,a_2,\cdots,a_n)$，记 $s(a)=\sum\limits_{i=1}^{n}k_ia_i$. 试证：有两个排列 b 和 c，$b\neq c$，使得 $n!\mid s(b)-s(c)$.

分析 所要证明的问题是 $n!\mid(s(b)-s(c))$. 自然地可联想到剩余类的性质，通过构造 $n!$ 的完全剩余类解题，根据题目特点，应采用反证法为宜.

证明 假设对任意两个不同的 b 和 c，均有 $s(b)\not\equiv s(c)(\mathrm{mod}\,n!)$，

则当 a 取遍所有 $1,2,\cdots,n$ 的 $n!$ 个排列时，$s(a)$ 遍历模 $n!$ 的一个完全剩余类，且每个剩余类恰经过一次，所以

$$\sum_a s(a)\equiv 1+2+\cdots+n!\ (\mathrm{mod}\,n!)\equiv\frac{n!\ (1+n!)}{2}(\mathrm{mod}\,n!), \quad ①$$

其中 $\sum\limits_a$ 表示对 a 取遍 $n!$ 个排列求和(下同).

另一方面

$$\sum_a s(a)=\sum_a\left(\sum_{i=1}^{n}k_ia_i\right)=\frac{n!\ (n+1)}{2}\sum_{i=1}^{n}k_i. \quad ②$$

由于 n 为大于 1 的奇数，则由①、②知

$$\frac{n!\ (1+n!)}{2}\equiv\frac{n!\ (n+1)}{2}(\mathrm{mod}\,n!)\equiv 0(\mathrm{mod}\,n!),$$

所以 $\dfrac{n!}{2}\equiv 0(\mathrm{mod}\,n!)$.

矛盾！故命题成立.

例 5 (1999 年中国数学奥林匹克)设 m 是给定的整数，试证：存在整数 a,b 和 k，其中 a,b 均为奇数，$k\geqslant 0$，使得 $2m=a^{19}+b^{99}+k\cdot 2^{1999}$.

证明 (1)设 $r,s\in\mathbf{N}_+$，其中 s 是奇数，如果 x 和 y 是模 2^r 互异的余数，那么 x^s、y^s 关于模 2^r 互不同余，这是因为

$x^s-y^s=(x-y)(x^{s-1}+x^{s-2}y+\cdots+y^{s-1})$,

并且 $x^{s-1}+x^{s-2}y+\cdots+xy^{s-2}+y^{s-1}$ 是奇数与 2^r 互质.

所以当 t 取遍 $\mathrm{mod}\,2^r$ 的简化剩余系时，t^s 也取遍 $\mathrm{mod}\,2^r$ 的简化剩余系.

(2)由(1)中的讨论，对于奇数 $2m-1$，必有奇数 a 使得 $2m-1=a^{19}+q\cdot 2^{1999}$. 对于 $b=1$ 有 $2m=a^{19}+b^{99}+q\cdot 2^{1999}$.

如果 $q\geqslant 0$，那么题目的结论已经得证.

如果 $q<0$，那么以 $a_0=a-h\cdot 2^{1999}$,

$$q_0=\frac{a^{19}-(a-h\cdot 2^{1999})^{19}}{2^{1999}}+q=\frac{(h\cdot 2^{1999}-a)^{19}+a^{19}}{2^{1999}}+q$$

代替 a 和 q，仍有：$2m=a_0^{19}+1^{99}+q_0\cdot 2^{1999}$,

当 h 足够大时，可使 $q_0\geqslant 0$,

于是原题目的结论得证.

例 6 对于任意整数 $n\geqslant 1$，试证：$2,2^2,2^{2^2},\cdots$ 自某项起各项对 n 同余.

分析 本题为 1991 年美国数学奥林匹克中的一道题，解法颇多，下面我们介绍两种.

证法一 为方便起见，令 $a_0=2^0$，$a_k=2^{a_{k-1}}(k\in\mathbf{N}_+)$,

显然当 $i\leqslant j$ 时，$a_i|a_j$.

由于在 $a_0,a_1,a_2,\cdots,a_n$ 这 $n+1$ 个数中必有两个数对模 n 同余，因此存在 $0\leqslant i<j\leqslant n$，使得 $a_i\equiv a_j(\bmod n)$.

若自然数 $s\geqslant j$，则有 $s-i-1\geqslant j-i-1\geqslant 0$，所以 $a_{j-i-1}|a_{s-i-1}$.

所以 $a_{j-i-1}|a_{s-i}$.

于是 $a_{j-i-1}|a_{s-i}-a_{s-i-1}$.

所以 $2^{a_{j-i-1}}-1|2^{a_{s-i}-a_{s-i-1}}-1$.

即为 $a_{j-i}|\frac{a_{s-i+1}}{a_{s-i}}-1$，所以 $a_{j-i}-a_0|a_{s-i+1}-a_{s-i}$.

又有 $2^{a_{j-i}-a_0}|2^{a_{s-i+1}-a_{s-i}}-1$，即 $\frac{2^{a_{s-i+1}-a_{s-i}}-1}{2^{a_{j-i}-a_0}-1}\in\mathbf{N}_+$.

所以 $\frac{a_{s-i+1}}{a_1}\cdot\frac{2^{a_{s-i+1}-a_{s-i}}-1}{2^{a_{j-i}-a_0}-1}=\frac{a_{s-i+2}-a_{s-i+1}}{a_{j-i+1}-a_1}\in\mathbf{N}_+$.

重复上述过程得 $\frac{a_{s-i+3}-a_{s-i+2}}{a_{j-i+2}-a^2}\in\mathbf{N}_+$,

……

$\frac{a_{s+1}-a_s}{a_j-a_i-a_2}\in\mathbf{N}_+$,

又 $n|a_j-a_i$.

所以 $a_{s+1}-a_s\equiv 0(\bmod n)$,

取 $s=j,j+1,j+2,\cdots$.

则有 $a_j\equiv a_{j+1}\equiv a_{j+2}\equiv\cdots(\bmod n)$,

所以自第 j 项起，每一项都对模 n 同余.

证法二 （用数学归纳法）

(1)当 $n=1$ 时，要证的结论显然成立；

(2)当 $n=2$ 时，要证的结论也成立.

对于 $n>2$，假设对所有小于 n 的自然数，要证的结论成立，对于 n，令 $n=2^k\cdot q$(q 为奇数).

如果 $q=1$，要证的结论也显然成立.

若 q 为大于 1 的奇数，记 $a_0=2^0$，$a_{i+1}=2^{a_i}$，($i=0,1,2\cdots$).

由于 $2^t\not\equiv 0\pmod{q}$，($0\leqslant t\leqslant q-1$)

于是存在 $0\leqslant i<j\leqslant q-1$，使得 $2^i\equiv 2^j\pmod{q}$，所以 $q\mid 2^j-2^i=2^i(2^{j-i}-1)$，

于是 $q\mid 2^{j-i}-1$.

记 $r=j-i$. 则 $1\leqslant r<q\leqslant n$，且 $2^r\equiv 1\pmod{q}$，

由归纳假设，存在 $i\in\mathbf{N}$，使得 $a_i\equiv a_{i_1}\pmod{n}$，对 $\forall\, i\geqslant i_1$.

于是 $a_i=a_{i_1}+rh$.

从而对 $\forall\, i\geqslant i_1$，有

$a_{i+1}=2^{a_i}=2^{a_{i_1}}\cdot(2^r)^h\equiv 2^{a_{i_1}}\pmod{q}\equiv a_{i_1+1}\pmod{q}$，

又显然存在 i_2，使当 $i\geqslant i_2$ 时，$2^k\mid a_i$，

令 $i_0=\max\{i_1+1,i_2\}$，

则对 $\forall\, i,j\geqslant i_0$，均有 $a_i\equiv a_j\pmod{2^kq}$，即 $a_i\equiv a_j\pmod{n}$.

于是对于 n，要证的结果也成立.

因此，对所有自然数 n，命题成立.

能力训练

1. 试写出模 30 的一个简化剩余系.

2. 对于任意的 $m\in\mathbf{N}_+$，试求和式 $s=\sum\limits_{d\mid m}\varphi(d)$.

3. 设 n 为奇数，试证：存在 $2n$ 个整数 $a_1,a_2,\cdots,a_n,b_1,b_2,\cdots,b_n$，使对任意一个整数 k，$0<k<n$，下列 $3n$ 个数 a_i+a_{i+1}，a_i+b_i，b_i+b_{i+k}($i=1,2,\cdots,n$，$a_{n+1}=a_1$，$b_{n+j}=b_j$)组成模 $3n$ 的完系.

4. 设 a,b 为两互质的正整数，试证：必有正整数 m,n，使 $ab\mid a^m+b^n-1$.

5. 使 $m,n\in\mathbf{N}_+$，且对任意的 $k\in\mathbf{N}_+$，有$(17k-1,m)=(17k-1,n)$. 试证：存在 $l\in\mathbf{Z}$，使得 $m=17^l\cdot n$.

6. 设 $d\in\mathbf{N}_+$，试证：$2d-1$，$5d-1$，$13d-1$ 这三个数中至少有一个不是完全平方数.

7. 若 n 是质数，试证：存在 $0,1,2,\cdots,n-1$ 的一个排列 $(a_1,a_2,\cdots,a_n)$，使得：a_1，a_1a_2，$\cdots$，$a_1a_2a_3\cdots a_n$ 组成模 n 的完系.

§2.3 欧拉定理、费马定理、威尔逊定理

知识扫描

1. **(欧拉定理)**若 $(a,m)=1$，则：$a^{\varphi(m)}\equiv1(\bmod m)$.

证明：设 $r_1,r_2,r_3,\cdots,r_{\varphi(m)}$ 是模 m 的一个简化剩余系，由于 $(a,m)=1$.

所以 $ar_1,ar_2,\cdots,ar_{\varphi(m)}$ 也是模 m 的一个简化剩余系.

所以 $ar_1\cdot ar_2\cdots ar_{\varphi(m)}\equiv r_1r_2\cdots r_{\varphi(m)}(\bmod m)$，

即 $m\mid(a^{\varphi(m)}-1)r_1r_2\cdots r_{\varphi(m)}$，

又 $(m,r_1r_2\cdots r_{\varphi(m)})=1$，所以 $m\mid a^{\varphi(m)}-1$.

所以 $a^{\varphi(m)}\equiv1(\bmod m)$.

2. **定义 6** 设 $m>1$ 是一个固定的整数 k，a 是与 m 互质的整数，则存在整数 k，$1\leqslant k\leqslant m$，使 $a^k\equiv1(\bmod m)$，我们将具有这一性质的最小正整数(仍记为 k)称为 a 模 m 的阶.

由 a 模 m 的阶(记为 k)的定义，易知 k 具有如下性质：

(1)设 $(a,m)=1$，k 是 a 模 m 的阶，u，v 是任意整数，则 $a^u\equiv a^v(\bmod m)$ 的充要条件是 $u\equiv v(\bmod k)$，特别地 $a^u\equiv1(\bmod k)$ 的充要条件是 $k\mid u$.

简证：充分性是显然的.

必要性：设 $u>v$，记 $l=u-v$，则由 $a^u\equiv a^v(\bmod m)$ 易知 $a^l\equiv1(\bmod m)$，设 $l=kq+r$，其中 $0\leqslant r<k$，使 $a^{kq}\cdot a^r\equiv1(\bmod m)$，所以 $a^r\equiv1(\bmod m)$.

由 $0\leqslant r<k$ 及 k 的定义知必有 $r=0$.

所以 $u\equiv v(\bmod m)$.

(2)设 $(a,m)=1$，a 模 m 的阶为 k，则数列 $a,a^2,\cdots,a^k,a^{k+1},\cdots$ 是模 m 的周期数列，其最小正周期为 k，而 k 个数 $a,a^2,\cdots,a^k$ 模 m 互不同余.

(3)设 $(a,m)=1$，则 a 模 m 的阶整除欧拉函数 $\varphi(m)$.

3. **(费尔马定理)**若 p 为素数，则 $a^p\equiv a(\bmod p)$.

证明：若 $(a,p)\neq1$，则 $p\mid a$，这时结论显然成立.

若$(a,p)=1$，则由欧拉定理$a^{\varphi(p)}\equiv 1\pmod{p}$，

又$\varphi(p)=p-1$，所以$a^{p-1}\equiv 1\pmod{p}$，

所以$a^p\equiv a\pmod{p}$.

定理证毕.

4.（**威尔逊定理**）若p为质数，则$(p-1)!\equiv -1\pmod{p}$.

证明：对于任意整数a，$1\leqslant a\leqslant p-1$，由裴蜀定理知存在整数$a'$，使得$aa'\equiv 1\pmod{p}$，不妨$1\leqslant a'\leqslant p-1$，则称$a'$为$a$的数论倒数.

若有整数b，满足$ba'\equiv 1\pmod{p}$，则$ba'a\equiv a\pmod{p}$，

所以$b\equiv a\pmod{p}$.

这就说明对于不同的整数a，$1\leqslant a\leqslant p-1$，对应着不同的数论倒数$a'$.

又如果整数a的数论倒数是它本身，则$a^2\equiv 1\pmod{p}$.

所以$a\equiv 1\pmod{p}$或$a\equiv -1\pmod{p}$.

从而当$p>2$时，$2,3,4,\cdots,(p-2)$恰好配成互为数论倒数的$\frac{p-3}{2}$对数，故它们的乘积$(p-2)!\equiv 1^{\frac{p-3}{2}}\pmod{p}\equiv 1\pmod{p}$，

所以$(p-1)!\equiv p-1\pmod{p}\equiv -1\pmod{p}$.

当$p=2$时，$(p-1)!\equiv -1\pmod{p}$.

故命题得证.

例题分析

例1 （2004年第36届加拿大数学奥林匹克）设p是奇质数，试证：$\sum\limits_{k=1}^{p-1}k^{2p-1}\equiv\frac{p(p+1)}{2}\pmod{p^2}$.

证明 因为$2\mid p-1$，故$\sum\limits_{k=1}^{p-1}k^{2p-1}=\sum\limits_{k=1}^{\frac{p-1}{2}}(k^{2p-1}+(p-k)^{2p-1})$，

由二项式定理得

$(p-k)^{2p-1}$

$=p^{2p-1}-C_{2p-1}^{1}p^{2p-2}\cdot k+\cdots-C_{2p-1}^{2p-3}p^2\cdot k^{2p-3}+C_{2p-1}^{2p-2}p\cdot k^{2p-2}-k^{2p-1}$.

所以$(p-k)^{2p-1}+k^{2p-1}$

$\equiv C_{2p-1}^{2p-2}p\cdot k^{2p-2}\pmod{p^2}$

$\equiv(2p-1)pk^{2p-2}\pmod{p^2}$，

对于 $1\leqslant k\leqslant p-1$，必有 $(k,p)=1$，

由费尔马定理：$k^{p-1}\equiv 1 \pmod p$，

所以 $(2p-1)k^{2p-1}\equiv(2p-1)\cdot 1^2\equiv -1 \pmod{p^2}$，

从而 $(2p-1)pk^{2p-1}\equiv -p \pmod{p^2}$，

所以 $\sum\limits_{k=1}^{p-1}k^{2p-1}\equiv -p\cdot\dfrac{p-1}{2} \pmod{p^2}\equiv p\dfrac{(p+1)}{2} \pmod{p^2}$。

评注 本题的关键在于将题中的各数两两配对，利用二项式展开后再利用费尔马定理。

例 2 （2002 年澳大利亚数学奥林匹克）设整数 n 和 q 满足 $n\geqslant 5$，$2\leqslant q\leqslant n$。试证：$q-1\left|\left[\dfrac{(n-1)!}{q}\right]\right.$。

证明 为了证明原命题，下面我们分以下两大类加以讨论：

(1) 当 q 为质数时，注意到 $2\leqslant q\leqslant n$。

①若 $q<n$，则易知 $q\mid(n-1)!$，$q-1\mid(n-1)!$。

又 $(q,q-1)=1$，所以 $q-1\left|\dfrac{(n-1)!}{q}\right.$，即 $q-1\left|\left[\dfrac{(n-1)!}{q}\right]\right.$。

此时命题成立。

②若 $q=n$，则由威尔逊定理，并注意到 q 为质数。

所以 $(q-1)!\equiv -1 \pmod q$，

所以 $\left[\dfrac{(n-1)!}{q}\right]=\left[\dfrac{(q-1)!}{q}\right]=\dfrac{(q-1)!+1}{q}-1$，

所以只需证 $q-1\left|\dfrac{(q-1)!+1}{q}-1\right.$。

又 $(q-1,q)=1$，

所以只需证 $q-1\left|q\left(\dfrac{(q-1)!+1}{q}-1\right)\right.\Leftrightarrow q-1\mid(q-1)!-(q-1)$。

上式显然成立。

所以此时命题成立。

(2) 当 q 为合数时。

①当 q 不是某质数的平方，则 q 必可写为 $ab(2\leqslant a<b)$。

注意到 $2\leqslant q\leqslant n$，所以 $2\leqslant a<b\leqslant n-1$。

所以 $a,b\in\{1,2,\cdots,n-1\}$，又 $a\neq b$，所以 $ab\mid(n-1)!$，即 $q\mid(n-1)!$，

所以 $\left[\dfrac{(n-1)!}{q}\right]=\dfrac{(n-1)!}{q}$。

所以只需证 $q-1\left|\dfrac{(n-1)!}{q}\right.$。

又$(q-1,q)=1$，只需证$q-1\mid(n-1)!$，

又$2\leqslant q\leqslant n$，所以$q-1\in\{1,2,\cdots,n-1\}$，

所以$q-1\mid(n-1)!$，故此时命题成立.

②若$q=p^2$（p为质数），下面说明$\left[\frac{(n-1)!}{q}\right]=\frac{(n-1)!}{q}$.

1°若$p=2$，则由于$n\geqslant5$，所以$4\mid(n-1)!$，所以$\left[\frac{(n-1)!}{q}\right]=\frac{(n-1)!}{q}$.

2°若$p\geqslant3$，则由于$n-1\geqslant q-1\geqslant p^2-1\geqslant3p-1>2p$，

所以$p,2p\in\{1,2,\cdots,n-1\}$.

所以$2p^2\mid(n-1)!$，所以$q\mid(n-1)!$.

所以$\left[\frac{(n-1)!}{q}\right]=\frac{(n-1)!}{q}$.

于是总有$\left[\frac{(n-1)!}{q}\right]=\frac{(n-1)!}{q}$. 同上易证此时命题也成立.

评注 本题并不很难，但想完全讨论清楚也不容易.

例3 （2003年第44届IMO试题）设p是质数. 试证：存在一个质数q，使对任意整数n，数n^p-p不是q的倍数.

证明 由于$\frac{p^p-1}{p-1}=1+p+p^2+\cdots+p^{p-1}\equiv1+p\pmod{p^2}$，

则$\frac{p^p-1}{p-1}$中至少有一个质因子q，满足$q\not\equiv1\pmod{p^2}$.

下面证明q为所求.

假设存在整数n，使得$n^p\equiv p\pmod{q}$，

则由q的选取，有$n^{p^2}\equiv p^p\equiv1\pmod{q}$.

另一方面，由费尔马小定理，有$n^{q-1}\equiv1\pmod{q}$（由于q为质数且$(n,q)=1$）.

由于$p^2\nmid q-1$，有$(p^2,q-1)\mid p$，

所以$n^p\equiv1\pmod{q}$.

所以$p\equiv1\pmod{q}\Rightarrow1+p+p^2+\cdots+p^{p-1}\equiv p\pmod{q}$.

由q的选取有$p\equiv0\pmod{q}$，矛盾！

所以命题得证.

例4 已知p为给定质数，求最小正整数m满足：(1) $1\leqslant m\leqslant p-1$；(2) $\sum_{k=1}^{p-1}k^m\equiv0\pmod{p}$.

解 (1)首先证明$m\neq p-1$.

对于$1\leqslant k\leqslant p-1$，由费尔马小定理$k^{p-1}\equiv1\pmod{p}$，

所以$\sum\limits_{k=1}^{p-1}k^{p-1}\equiv\sum\limits_{k=1}^{p-1}1 \pmod p\equiv p-1 \pmod p$.

所以 $p\nmid\sum\limits_{k=1}^{p-1}k^{p-1}$. 所以 $m\neq p-1$.

(2)下面再证明 $m=p-2$ 满足要求.

考虑同余方程 $x^{p-2}\equiv1 \pmod p$，该方程至多只有 $p-2$ 个解，于是存在 $a\in\{1,2,\cdots,p-1\}$，使得：$a^{p-2}\not\equiv1 \pmod p$.

又 $1,2,\cdots,p-2,p-1$ 组成模 p 的缩系，

而显然$(a,p)=1$，所以 $a,2a,\cdots,a(p-2),a(p-1)$也组成模 p 的缩系.

所以$\sum\limits_{k=1}^{p-1}k^{p-2}\equiv\sum\limits_{k=1}^{p-1}(ka)^{p-2} \pmod p$，即 $p\left|(a^{p-2}-1)\sum\limits_{k=1}^{p-1}k^{p-2}\right.$，

又 $p\nmid a^{p-2}-1$，p 为质数. 所以$(p,a^{p-2}-1)=1$.

所以 $p\left|\sum\limits_{k=1}^{p-1}k^{p-2}\right.$.

所以满足要求的 m 的最大值为 $p-2$.

评注 用类似的方法可以证明：(p 为质数). $p\left|\sum\limits_{k=1}^{p-1}k^{m}\right.\Leftrightarrow p-1\nmid m$.

例 5 (2006 年国家集训队测试题)求所有的正整数对(a,n)，使得 $n\mid(a+1)^n-a^n$.

证法一 首先易知$(a,n)=(a,1)$是满足要求的，当 $n\geqslant2$ 时，易知 n 为奇数且$(n,a)=(n,a+1)=1$，由条件：

$(a+1)^n\equiv a^n \pmod n$. ①

因为$(a,n)=1$，

由裴蜀定理，存在 $m\in\mathbf{N}_+$，使得 $a+1\equiv ma \pmod n$，

所以$(a+1)^n\equiv m^n a^n \pmod n$， ②

由①，②得：$a^n\equiv m^n a^n \pmod n$.

又$(a^n,n)=1$，所以 $m^n\equiv1 \pmod n$，

设 p 是 n 的最小质因数，则 $m^n\equiv1 \pmod p$.

又$(m,p)=1$，由费尔马小定理 $m^{p-1}\equiv1 \pmod p$，所以 $p\mid m^{(n,p-1)}-1$.

又 p 是 n 的最小质因数，

所以$(n,p-1)=1$，所以 $p\mid m-1$.

所以 $a+1\equiv am \pmod p\equiv a \pmod p$.

所以 $p\mid1$ 矛盾！

所以满足要求的(a,n)为$(a,1)(a\in\mathbf{N}_+)$.

证法二 当 $n\geqslant2$ 时，设 p 为 n 的最小质因数，

则$(n,p-1)=1$，由裴蜀定理

存在 $u,v\in\mathbf{N}_+$，满足 $nu-(p-1)v=1$，

又 $p|(a+1)^n-a^n$，所以 $p|(a+1)^{nu}-a^{nu}$，

即 $p|(a+1)^{(p-1)v+1}-a^{(p-1)v+1}$. ①

又由费马小定理 $(a+1)^{p-1}\equiv a^{p-1}\equiv 1(\bmod p)$，

所以由①知 $p|(a+1)-a$ 矛盾！

所以 $n=1$.

综上所述满足要求的 (a,n) 为 $(a,1)(a\in\mathbf{N}_+)$.

评注 本题解法颇多，在下面的第 6 章中我们将用“无穷递降法”给出另一种解法.

例 6 (1999 年第 40 届 IMO 试题)确定所有的正整数对 (n,p)，满足：p 是一质数，$n\leqslant 2p$ 且 $(p-1)^n+1$ 能够被 $(1,p)$ 整除.

分析 这道题实际上是证明 $(p-1)^n\equiv -1(\bmod n^{p-1})$，很容易联想到利用阶的思想.

解 $p=2$ 时，只有整数 $n=1,2$ 满足要求.

下面考虑 p 为不小于 3 的奇质数的情形：

这时，$(p-1)^n+1$ 为奇数，于是 n 只能为奇数. 先设 $n>1$，设 n 的最小质因数为 $q\geqslant 3$，则 n 可以表示成 $n=q^k\cdot s$，其中 $q\nmid s$，$k\geqslant 1$，s 为奇数，且 s 的每个质因数(如果 $s\neq 1$)均大于 q.

于是由 $(p-1)^n\equiv -1(\bmod n^{p-1})$ 知：$(p-1)^n\equiv -1(\bmod q)$.

由费马小定理：$(p-1)^{q^k}\equiv p-1(\bmod q)$，所以 $(p-1)^s\equiv -1(\bmod q)$.

设 l 为 $p-1$ 对模 q 的阶，则 $(p-1)^l\equiv 1(\bmod q)$，

又 $(p-1)^s\equiv -1(\bmod q)$，$(p-1)^{2s}\equiv 1(\bmod q)$，

$(p-1)^{q-1}\equiv 1(\bmod q)$，所以 $l|2s$，$l|q-1$，$l\nmid s$，

所以 l 为偶数，且 $l|(2s,q-1)$.

由 q 及 s 的取法，所以 $(2s,q-1)=2$，

所以 $l=2$. 所以 $q|(p-1)^2-1$.

又 $p-1\not\equiv 1(\bmod q)$，所以 $q|(p-1)+1$. 所以 $q=p$.

故 $p|n$，又 $n\leqslant 2p$，所以 $n=p$(注意 n 为奇数).

所以 $(p-1)^p\equiv -1(\bmod p^{p-1})$.

若 $p\geqslant 5$，则 $p^3|p^{p-1}$，所以 $(p-1)^p\equiv -1(\bmod p^3)$.

$$
\begin{aligned}
\text{又}(p-1)^p+1&=\sum_{j=3}^{p}C_p^j(-1)^{p-j}p^j+C_p^1(-1)^{p-2}p^2+p^2\\
&\equiv p^2(\bmod p^3).
\end{aligned}
$$

矛盾！

所以 $p=3$，此时 $(n,p)=(3,3)$.

又易知 $(1,p)$ 是满足要求的.

所以满足要求的一切解为(2,2),(3,3),(1,p)(p 为质数).

评注 设 p 为 n 的最小质因数是一种非常有用的技巧,由此即得$(p-1,n)=1$,这与费马小定理及模阶的思想结合是解题的一种常用的手段.

例 7 (第 16 届巴尔干数学奥林匹克竞赛)设 $p>3$ 为素数,使 $3\mid p-2$. 记 $S=\{y^2-x^3-1\mid x,y\in \mathbf{Z},0\leqslant x,y\leqslant p-1\}$. 试证:$S$ 中至多有 $p-1$ 个元素是 p 的倍数.

分析 由费尔马小定理可以推得:若 $1\leqslant m<n\leqslant p-1$,则 $m^3\not\equiv n^3 \pmod p$,这里 $p>3$ 是质数且 $p\equiv 2 \pmod 3$,再由完全剩余系的知识推得结论.

证明 先证一引理:质数 $p>3$ 且 $p\equiv 2 \pmod 3$,若 $x^3\equiv y^3 \pmod p$,则 $x\equiv y \pmod p$.

引理的证明:(1)若 x,y 有一个为 p 的倍数则易知此时引理成立.

(2)若 $p\nmid x$,$p\nmid y$,则由于 p 为质数,于是$(x,p)=(y,p)=1$.

于是由费尔马小定理:

$x^{p-1}\equiv y^{p-1}\equiv 1 \pmod p$.

又 $x^3\equiv y^3 \pmod p$,$p\equiv 2 \pmod 3$,

所以 $x^{p-2}\equiv y^{p-2} \pmod p$.

又 $p\mid x^{p-1}-y^{p-2}\cdot y$,所以 $p\mid x^{p-1}-x^{p-2}\cdot y$.

即 $p\mid x^{p-2}(x-y)$,又$(p,x^{p-2})=1$,

所以 $p\mid x-y$. 所以 $x\equiv y \pmod p$.

故引理得证.

下面证明原命题:

由引理知,当 x 取遍模 p 的完系时,x^3 也取遍模 p 的完系,于是对于某个固定的 $y\in\{0,1,2,\cdots,p-1\}$,恰有一个 $x\in\{0,1,2,\cdots,p-1\}$,使得 $p\mid y^2-x^3-1$. 注意到 y 共有 p 种选择,于是 S 中至多有 p 个数是 p 的倍数.

又 $1^2-0^3-1=0\in S$,$3^2-2^3-1=0\in S$,

所以 S 中至多有 $p-1$ 个数是 p 的倍数.

证毕.

例 8 设正整数 $k\geqslant 2$,$n_1,n_2,\cdots,n_k$ 是满足条件 $n_2\mid 2^{n_1}-1$,$n_3\mid 2^{n_2}-1$,$\cdots$,$n_k\mid 2^{n_{k-1}}-1$,$n_1\mid 2^{n_k}-1$ 的一组正整数,试证:$n_1=n_2=\cdots=n_k=1$.

证明 先证一引理:若 $m,n>1$ 且满足 $m\mid 2^n-1$,设 m,n 的最小质因数为 q_1,q_2,则:$q_1>q_2$.

引理的证明:由条件 $m\mid 2^n-1$,又 $q_1\mid m$,

所以 $q_1\mid 2^n-1$,显然$(q_1,2)=1$.

于是由费尔马小定理得:$q_1\mid 2^{q_1-1}-1$,又 $q_1\mid 2^n-1$,

所以 $q_1\mid 2^{(n,q_1-1)}-1$.

若 $q_1 \leqslant q_2$，则由 q_2 的定义易知 $(n, q_1-1)=1$，

所以 $q_1 \mid 2^1-1$，矛盾！

所以 $q_1 > q_2$.

所以引理得证.

下面证明原命题：

(1)若 $n_1, n_2, \cdots, n_k$ 中存在一个数不为 1，不妨设 $n_2 \neq 1$，则由 $n_2 \mid 2^{n_1}-1 \Rightarrow n_1 \neq 1 \Rightarrow n_k \neq 1 \Rightarrow n_{k-1} \neq 1 \Rightarrow \cdots \Rightarrow n_3 \neq 1$，所以 $n_1, n_2, \cdots, n_k$ 全不为 1 且为奇数.

于是可设 n_i 的最小质因数为 $p_i(1 \leqslant i \leqslant k)$，

又 $n_2 \mid 2^{n_1}-1, n_3 \mid 2^{n_2}-1, \cdots, n_k \mid 2^{n_{k-1}}-1, n_1 \mid 2^{n_k}-1$，

由引理易知：$p_2 > p_1 > p_k > p_{k-1} > p_{k-2} > \cdots > p_3 > p_2$，矛盾！

所以 $n_1 = n_2 = \cdots = n_k = 1$.

证毕.

例 9 （2006 年国家集训队试题）试证：对任给正整数 m, n，总存在正整数 k，使得 2^k-m 至少有 n 个不同的素因子.

证明 固定 m，不妨设 m 为奇数. 我们将证明对任何正整数 n，总存在 k_n，使得 $2^{k_n}-m$ 至少有 n 个不同素因子. ①

下面用数学归纳法证明①：

(1)当 $n=1$ 时，$2^{3m}-m$ 显然至少有一个素因子；

(2)假设 $2^{k_n}-m$ 至少有 n 个不同素因子，令 $A_n=2^{k_n}-m$，则 $(A_n, 2)=1$，且

$2^{k_n+\varphi(A_n^2)}-m \equiv 2^{k_n}-m \equiv A_n(\bmod A_n^2)$，所以 $A_n \mid 2^{k_n+\varphi(A_n^2)}-m$，

取质数 $p \left| \dfrac{2^{k_n+\varphi(A_n^2)}-m}{A_n} \right.$，由 $\dfrac{2^{k_n+\varphi(A_n^2)}-m}{A_n} \equiv 1(\bmod A_n)$ 知 $p \nmid A_n$.

所以 $2^{\varphi(A_n^2)+k_n}-m$ 至少有 $n+1$ 个不同素因子.

由数学归纳法知结论成立.

评注 事实上，本题的解题思路非常容易考虑到，本题在集训题中的得分率奇高，就说明了这一点.

能力训练

1. 求最小的正整数 k，使得存在正整数 m, n，满足 $k=19^n-5^m$.

2. 设 $m, n \in \mathbf{N}_+$，m 为奇数，$(m, 2^n-1)=1$. 试证：和数 $1^n+2^n+\cdots+m^n$ 是 m 的倍数.

3. 设 $m>n\geqslant 1$，求 $m+n$ 的最小值，满足：$1000\mid 1978^m-1978^n$.

4. 对于任意的非负整数 n，$19\cdot 8^n+17$ 为合数.

5. 求正整数 n，使得 $\frac{2^n+1}{n^2}$ 为整数.

6. 求所有素数对 (p,q)，使得 $pq\mid (5^p-2^p)(5^q-2^q)$.

7. 设 p,q 是两个奇质数，$p>q$. 试证：对任意的正整数 m，$pq\nmid m^{p-q}+1$.

8. 设 $n>1$ 为正整数，试证：$n\nmid 2^n-1$.

9. 确定满足以下要求的一切大于 1 的整数 n，使得：对所有与 n 互质的数 $a,b\in \mathbf{Z}$，$a\equiv b(\bmod n)\Leftrightarrow ab\equiv 1(\bmod n)$.

10. 试求满足以下条件的全部质数 p：对任一质数 $q<p$，若 $p=kq+r$，$0\leqslant r<q$，则不存在大于 1 的整数 a，使得 $a^2\mid r$.

11. 求所有正整数 x,y,z，使得：$xy(\bmod z)\equiv yz(\bmod x)\equiv zx(\bmod y)=2$.

12. 已知 p 为大于 3 的奇质数，$a>b>1$. 试证：$C_{pa}^{pb}\equiv C_a^b(\bmod p^3)$.

13. 试证：存在 $a\in \mathbf{Z}$，使得 $a^2\equiv -1(\bmod p)$（p 为奇质数）的充要条件是 $p\equiv 1(\bmod 4)$.

14. 设 S 是所有满足下列条件的质数 p 组成的集合：$\frac{1}{p}$ 的小数部分中最小循环节中数码的个数是 3 的倍数，即对于每个 $p\in S$，存在最小的正整数 $r=r(p)$，使 $\frac{1}{p}=0.a_1a_2\cdots$
$a_{3r}a_1a_2\cdots a_{3r}\cdots$

对于每个 $p\in S$ 和任意整数 $k\geqslant 1$，定义 $f(k,p)=a_k+a_{k+r(p)}+a_{k+2r(p)}$.

(1) 试证：集合 S 中有无穷多个质数；

(2) 对于 $k\geqslant 1$ 及 $p\in S$，求 $f(k,p)$ 的最大值.

15. 任意给定 $h=2^r$（r 是非负整数），求满足以下条件的所有自然数 k：对每个这样的 k，存在奇自然数 $m>1$ 和自然数 n，使得：$k\mid m^h-1$，$m\mid n^{\frac{m^h-1}{k}}+1$.

第三章　同余方程与平方剩余

§3.1　一次同余方程与孙子定理

知识扫描

本节将讨论一次同余方程和由此引申出的重要定理——孙子定理,首先介绍若干概念.

设整系数多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$,若有整数 c,满足 $f(c)\equiv 0(\bmod m)$①,则称 c 是满足同余方程①的解,记作 $x\equiv c(\bmod m)$. 当且仅当 c_1,c_2 均是①的解,且 c_1 与 c_2 模 m 不同余时,我们称 c_1,c_2 是①的两个不同解. 一般情况,我们说同余方程①的解数,即指 $\bmod m$ 两两不同余的解的个数.

最简单的同余方程是一次同余方程

$$ax\equiv b(\bmod m),m\nmid a. \quad ②$$

同余方程②有解的充要条件是 $(a,m)\mid b$(请读者自行证明,关键在利用带余除法及最大公约数理论). 特别地,在 $(a,m)=1$ 时,②必有解. 事实上由第二章§2.2知:$(a,m)=1$,x_i 遍历模 m 的一组完系时,ax_i 也遍历模 m 的一组完系($i=1,2,\cdots,m$). 因此,有且仅有一个 $r_0=x_i$ 使得 $ax_i\equiv ar_0\equiv b(\bmod m)$,即同余方程②至多一个解. 进一步,一定存在 a' 使得 $a'\cdot a\equiv 1(\bmod m)$(例如取 $a'\equiv a^{\varphi(m)-1}$),于是 $x\equiv a^{\varphi(m)-1}b(\bmod m)$,即为 $(a,m)=1$ 时②的解. 更进一步,我们可求出②的通解为 $x\equiv x_0+\frac{m}{(a,m)}t(\bmod m)$,$t=0,1,\cdots,(a,m)-$

1，其中 x_0 是②的一个特解.

设 $k>1,a_i,b_i$ 是整数，m_i 是正整数，$i=1,2,\cdots,k$，则称下面这 k 个同余式

$$\begin{cases}a_1x+b_1\equiv 0(\bmod m_1)\\ a_2x+b_2\equiv 0(\bmod m_2)\\ \cdots\\ a_kx+b_k\equiv 0(\bmod m_k)\end{cases} \quad ③$$

为一次同余方程组，显然，③中若有一个同余方程无解，则③无解. 从而在③有解时，③中每个同余方程都有解，可将求③的解转化为求若干个下述方程的解.

$$\begin{cases}x\equiv c_1(\bmod m_1)\\ x\equiv c_2(\bmod m_2)\\ \cdots\\ x\equiv c_k(\bmod m_k)\end{cases} \quad ④$$

讨论一下④的本质，先看 $k=2$ 的情况.

定理 1 设 $m=m_1m_2$，$x_i^{(1)}$ 是模 m_1 的完全剩余系，$x_j^{(2)}$ 是模 m_2 的完全剩余系，则 $x_{ij}=x_i^{(1)}+m_1x_j^{(2)}$ 是模 m 的完全剩余系. 即 $x^{(1)}$，$x^{(2)}$ 分别遍历模 m_1，模 m_2 的完全剩余系时，$x=x^{(1)}+m_1x^{(2)}$ 遍历模 $m=m_1m_2$ 的完全剩余系.

证明 此时 x_{ij} 共有 $m=m_1m_2$ 个数，因而只需证明它们对 m 两两不同系.

若 $x_{i_1}^{(1)}+m_1x_{j_1}^{(2)}\equiv x_{i_1j_1}\equiv x_{i_2j_2}\equiv x_{i_2}^{(1)}+m_1x_{j_2}^{(2)}(\bmod m_1m_2)$，

则必有 $x_{i_1}^{(1)}\equiv x_{i_2}^{(1)}(\bmod m_1)$，

从而必有 $i_1=i_2$，$x_{i_1}^{(1)}=x_{i_2}^{(1)}$（因为 $x_i^{(1)}$ 在同一个模 m 的完系中取值）.

进而得 $m_1x_{j_1}^{(2)}\equiv m_1x_{j_2}^{(2)}(\bmod m_1m_2)$，

即 $x_{j_2}^{(2)}\equiv x_{j_1}^{(2)}(\bmod m_2)$.

同理有 $j_1=j_2$，$x_{j_1}^{(2)}=x_{j_2}^{(2)}$，定理得证.

定理 1 刻画了完系的某种结构，表明大模 $m=m_1m_2$ 的完系，可以表示为两个较小的模的完系的"组合". 同时我们应注意到，$(m_1,m_2)=1$，$x^{(1)}$ 遍历模 m_1 的完系时，$m_2x^{(1)}$ 也遍历模 m_1 的完系（这个性质的确是常用并且有用的），这样我们立即得到定理 2.

定理 2 设 $m=m_1m_2$，$(m_1,m_2)=1$，$x^{(1)}$，$x^{(2)}$ 分别遍历模 m_1，m_2 的完全剩余系，则 $x_{ij}=m_2x_i^{(1)}+m_1x_j^{(2)}$ 遍历模 m_1m_2 的完全剩余系.

进一步分析，我们可以得到一般情形的刻画.

定理 3 设 $m=m_1m_2\cdots m_k$，$m_1,m_2,\cdots,m_k$ 两两既约，再设 $m=m_j\cdot M_j(1\leqslant j\leqslant k)$ 及 $x=M_1x^{(1)}+M_2x^{(2)}+\cdots+M_kx^{(k)}$，那么当 $x^{(1)}$，$x^{(2)}$，$\cdots$，$x^{(k)}$ 分别遍历模 $m_1,m_2,\cdots,m_k$ 的完全剩余系时，x 遍历模 $m=m_1m_2\cdots m_k$ 的完全剩余系.

证明 $k=2$ 时，即定理 2.

设 $k=n(n\geqslant 2)$ 时定理成立.

当 $k=n+1$ 时,

记 $\overline{x}^{(n)}=\frac{m}{m_1 m_{n+1}}x^{(1)}+\cdots+\frac{m}{m_n m_{n+1}}x^{(n)}$,

我们有 $x=m_{n+1}\overline{x}^{(n)}+\frac{m}{m_{n+1}}x^{(n+1)}$.

由上两式及 $k=2$ 成立,即证明了结论. 至此,我们较清楚地展示了"大模"$m=m_1m_2\cdots m_k$是如何被较小的模 $m_1,m_2,\cdots$刻画的.

下面给出"孙子定理"(亦称"中国剩余定理").

定理(孙子定理)

设 $m_1,m_2,\cdots,m_k$ 是两两既约的正整数,那么同余方程④的解是

$x\equiv M_1M_1^{-1}c_1+M_2M_2^{-1}c_2+\cdots+M_kM_k^{-1}c_k(\bmod m)$,

这里 $m=m_1m_2\cdots m_k, m=m_jM_j(1\leqslant j\leqslant k)$,

$M_j^{-1}\cdot M_j\equiv 1(\bmod m_j)\quad(1\leqslant j\leqslant k)$.

孙子定理依旧刻画的是剩余系的结构,请读者将其与定理3进行对比,可以看出,孙子定理是着重刻画一组已定下的较小模的剩余类与一个较大的模的某个剩余类间的关系,而定理3则是讨论宏观上它们间的联系. 中国剩余定理在做题时的指导在于它能断定同余方程组④在模两两互素时,一定有解. 甚至有些时候,我们并不关心解是什么,而关注是否有解,怎样使其有解.

例题分析

例1 解同余方程组

$$\begin{cases}x\equiv 1(\bmod 3)\\x\equiv -1(\bmod 5)\\x\equiv 2(\bmod 7)\\x\equiv -2(\bmod 11)\end{cases}$$

解 取 $m_1=3,m_2=5,m_3=7,m_4=11$,这时 $M_1=5\cdot 7\cdot 11, M_2=3\cdot 7\cdot 11, M_3=3\cdot 5\cdot 11, M_4=3\cdot 5\cdot 7$.

又由 $M_1\equiv(-1)\cdot(1)\cdot(-1)\equiv 1(\bmod 3)$,

所以 $1\equiv M_1M_1^{-1}\equiv M_1^{-1}(\bmod 3)$,可取 $M_1^{-1}=1$.

由 $M_2\equiv(-2)\cdot(2)\cdot(1)\equiv 1(\bmod 5)$,

所以 $1\equiv M_2M_2^{-1}\equiv M_2^{-1}(\bmod 5)$,可取 $M_2^{-1}=1$.

由 $M_3\equiv 3\times 5\times 4\equiv 4(\mathrm{mod}7)$，

所以 $1\equiv M_3M_3^{-1}\equiv 4M_3^{-1}(\mathrm{mod}7)$，可取 $M_3^{-1}=2$.

由 $M_4\equiv 3\times 5\times 7\equiv 4\times 7\equiv 6(\mathrm{mod}11)$，

所以 $1\equiv M_4M_4^{-1}\equiv 6M_4^{-1}(\mathrm{mod}11)$，可取 $M_4^{-1}=2$.

由孙子定理知同余方程的解为

$x=(5\cdot 7\cdot 11)\cdot 1\cdot 1+(3\cdot 7\cdot 11)\cdot 1\cdot(-1)+(3\cdot 5\cdot 11)\cdot 2\cdot 2+(3\cdot 5\cdot 7)\cdot 2\cdot(-2)(\mathrm{mod}3\cdot 5\cdot 7\cdot 11)$，

即 $x\equiv 394(\mathrm{mod}1155)$.

评注 运用孙子定理时，必须确保模是两两互质的，当某两个模不互质时，要将同余方程组进行变形，这将在练习中出现.

例 2 任意给定的整数 n，证明：一定存在 n 个连续正整数，其中每一个都有大于 1 的平方因子.

证明 由于素数有无穷多个，因而对任意的 n，均可选出 n 个不同的素数 $p_1,p_2,\cdots,p_n$.

考虑同余方程组 $x\equiv -i(\mathrm{mod}p_i^2)$，由于 $p_1^2,p_2^2,\cdots,p_n^2$ 显然两两互素，由中国剩余定理知上述同余方程组有解，于是 $x+1,x+2,\cdots,x+n$ 这 n 个数分别被 $p_1^2,p_2^2,\cdots,p_n^2$ 整除，问题得证.

评注 在构造同余式时，选择质数的某些形式作为模是十分有效的，再看一个构造的例子.

例 3 能否找到含有 2005 个自然数的集合，使(1)S 中任意两数互素；(2)S 中任意 k $(k\geqslant 2)$个数的和为合数.

分析与解 2005 显然是“年份数据”，为此考虑 n 个元素的集合，由于同时满足(1)(2)两个要求不易找到一个直接的构造，只能一步步地探索.

对于满足(1)的 n 元集是容易构造，故设我们已找到一个满足(1)的集合 $\{x_1,x_2,\cdots,x_n\}$，下面关心怎样更进一步约束或者变动该集合，使其满足(2)，然而这不易做到，其难处在于(2)中“任意 k 个数的和”不好控制. 我们当然希望需要控制的“k 数和”变少，自然想到了“归纳构造”. 我们设 $\{x_1,x_2,\cdots,x_n\}$ 已经满足了(1)(2)，下面用 $x_1,x_2,\cdots,x_n$ 推出 x_{n+1} 应为何物. $\{x_1,x_2,\cdots,x_{n+1}\}$ 中含 x_{n+1} 的“k 数和”有 2^n-1 个($k\geqslant 2$)，设这些和为 $S_1,S_2,\cdots,S_{2^n-1}$，则 $T_1=S_1-x_{n+1},T_2=S_2-x_{n+1},\cdots,T_{2^n-1}=S_{2^n-1}-x_{n+1}$ 均为定值(它们均为 $x_1,x_2,\cdots,x_n$ 中的几个元素之和)，我们想让 $x_{n+1}+(S_1-x_{n+1}),x_{n+1}+(S_2-x_{n+1}),\cdots,x_{n+1}+(S_{2^n-1}-x_{n+1})$ 均为合数，这利用中国剩余定理是容易办到的，因为同余方程组：$x_{n+1}\equiv x_{n+1}-S_i\equiv -T_i(\mathrm{mod}p_i)$ 是有解的，其中 $p_1,p_2,\cdots,p_{2^n-1}$ 是两两互素的数，且 $p_i\neq 1$ $(i=1,2,\cdots,2^n-1)$. 这样我们便让 $\{x_1,x_2,\cdots,x_{n+1}\}$ 满足了(2).

回头看此时$\{x_1,x_2,\cdots,x_{n+1}\}$是否满足(1)？这一点并不确定，从而应当控制一下$p_i$的值.由于$x_1,x_2,\cdots,x_n$已经两两互质，所以若$x_{n+1}$能表示为$kx_1\cdot x_2\cdots x_n+1$的形式，则$x_{n+1},x_1,x_2,\cdots,x_n$两两互素，这实际上是要求$x_{n+1}\equiv 1(\bmod x_1x_2\cdots x_n)$，至此，怎样控制$p_i$已经非常明确了，我们只需$2^n-1$个质数$p_1,p_2,\cdots,p_{2^n-1}$，它们均与$a_1\cdot a_2\cdot\cdots\cdot a_n$互素，考虑$2^n$个同余式$x_{n+1}\equiv -T_i(\bmod p_i)(i=1,2,\cdots,2^n-1)$，$x_{n+1}\equiv 1(\bmod a_1\cdot a_2\cdot\cdots\cdot a_n)$，由中国剩余定理，这样的$x_{n+1}$存在.至此完成了归纳构造.

特别地，$n=2005$时我们能找到一个满足(1)(2)的集合.

例4 求具有下述性质的n，存在$0,1,2,\cdots,n-1$的排列$(a_1,a_2,\cdots,a_n)$使得$a_1,a_1a_2,a_1a_2a_3,\cdots,a_1a_2\cdots a_n$恰好构成模$n$的完全剩余系.

解 首先实验几个较小的n，

$n=1$时，显然满足条件，

$n=2$时，$(1,0)$满足条件，

$n=3$时，$(1,2,0)$满足条件，

$n=4$时，$(1,3,2,0)$满足条件，

$n=5$时，$(1,2,4,3,0)$满足条件，

$n=6$时，经试验没有满足条件的$(a_1,a_2,\cdots,a_6)$，

$n=7$时，$(1,6,2,4,5,3,0)$满足条件，

$n=8$时，经试验没有满足条件的$(a_1,a_2,\cdots,a_8)$.

通过上述实验，我们猜测n为质数时，均是满足条件，尽管这可能是不全面的.

下面先证明这个结论.

事实上，对任意质数p，由中国剩余定理，对每个$k=2,3,\cdots,p$，存在b_k，使得$b_k\equiv 0(\bmod k-1)$，$b_k\equiv k(\bmod p)$，用a_k表示$c_k=\frac{b_k}{k-1}$被n除的余数$k=2,3,\cdots,p$，则$b_k\equiv a_k(k-1)\equiv k(\bmod p)$.

令$a_1=1$，下面证明$a_1,a_2,\cdots,a_p$互不相同(从而$(a_1,a_2,\cdots,a_p)$是$0,1,2,\cdots,p-1$的一个排列).

事实上，由$a_p(p-1)\equiv p\equiv 0(\bmod p)$，有$a_p=0$，故$a_1\neq a_p$.又当$k=2,3,\cdots,p-1$时，$a_k(k-1)\equiv k(\bmod p)$，故$p\nmid a_k(k-1)$，所以$p\nmid a_k$，这表明$a_k\neq a_p$.

若存在$k,l,2\leqslant k<l\leqslant p-1$，使得$a_k=a_l=a$，则

$a_l(l-1)k=a(kl-k)\equiv kl(\bmod p)$，

$a_k(k-1)l=a(kl-l)\equiv kl(\bmod p)$，

从而$a(k-l)=a(kl-l)-a(kl-k)\equiv 0(\bmod p)$.

这说明$p|a$，与$a_k\neq 0$矛盾.

若存在$k,2\leqslant k<n$，使得$a_k=a_1$，则$k-1=a_k(k-1)\equiv k(\bmod p)$，

这说明 $p|(-1)$，矛盾.

以上说明了 $(a_1,a_2,\cdots,a_n)$ 的确为 $0,1,2,\cdots,n-1$ 的排列，同时 $a_1\cdot a_2\cdot\cdots\cdot a_k\equiv(2-1)a_2a_3\cdots a_k\equiv 2a_3\cdots a_k=(3-1)a_3\cdots a_k\equiv\cdots\equiv(k-1)a_k\equiv k(\mathrm{mod}\,p)$，

所以当 n 为质数 p 时满足条件.

接下来，我们考虑一下其他可能情形，稍做分析，即可知对大于 4 的合数 n，n 均不满足题意.

若 $n=p^2$，记 $q=2p<n$；否则 $n=pq$，$1<p<q<n$，在这两种情况下，均有 $pq\equiv 0(\mathrm{mod}\,n)$ 且 $p,q\in\{2,3,\cdots,n-1\}$.

设 $(a_1,a_2,\cdots,a_n)$ 是满足条件的序列，则

$k=1,2,\cdots,n-1$ 时，$a_k\neq 0$，否则 $a_1a_2\cdots a_k\equiv 0(\mathrm{mod}\,n)$，

$a_1a_2\cdots a_{k+1}\equiv 0(\mathrm{mod}\,n)$，

于是，存在 $k,l<n$，使 $a_k=p$，$a_l=q$.

记 $m=\max\{k,l\}<n$，则 $a_ka_l|a_1a_2\cdots a_m$.

因此有 $a_1a_2\cdots a_m\equiv 0(\mathrm{mod}\,n)$，$a_1a_2\cdots a_{m+1}\equiv 0(\mathrm{mod}\,n)$ 矛盾！

这便证明 $n>4$ 且为合数时，n 并不满足条件.

所以，符合条件的 n 应为 1，4 及所有质数.

例 5 证明：存在一个正整数 n，使得对于任意正整数 k，$n\cdot 2^k+1$ 均为合数.

分析与解 题中要求对变化着的 k，使得 $n\cdot 2^k+1$ 均为合数，有两种自然的想法：(1)考虑该式是否能够因式分解；(2)证明该式恒为某个质数或某几个质数的倍数.

对于(1)，似乎不容易做到，因为要使该式能进行分解的 n 总要求和 k 有些联系，如 $n=2^{3k+1}$，但这不符合题中"n 为定数"的要求，把角度转向(2)，这看似好像很容易做到，这是因为我们只需考虑 2^k 模一些质数得到的余数，再利用孙子定理确定 n 的值.

下面就关心 2^k 模质数后的余数. 为了满足题意，我们要确保两件事，即 k 取遍所有正整数时，我们只能用有限个质数做模（否则无法用中国剩余定理），同时对于每个作为模的质数 p_{i_0}，2^k 模 p_{i_0} 只能出现一种余数（否则这样的数不存在），而这不容易做到，其难处在于我们能否找到几组剩余类，使得对任意的 k 都必属于其中之一，对于上述这种剩余类，我们称其为"同余覆盖式". 分析表明，它是存在的，且不只一组，下面给出一组，希望读者能将其记住.

$k\equiv 1(\mathrm{mod}\,2)$， ⑤

$k\equiv 1(\mathrm{mod}\,3)$， ⑥

$k\equiv 2(\mathrm{mod}\,4)$， ⑦

$k\equiv 4(\mathrm{mod}\,8)$， ⑧

$k\equiv 0(\mathrm{mod}\,12)$， ⑨

$k\equiv 8\pmod{24}$. ⑩

请自行证明对任意的 k,它至少适合上述 6 个式子中的一个.

至此,我们可看到:若 k 满足⑤,

则 $n\cdot 2^k+1=k\cdot 2^{2m+1}+1=2k\cdot 4^m+1\equiv 2k+1\pmod 3$,

同样,若 k 分别满足⑥⑦⑧⑨⑩式时,

$k\cdot 2^n+1\equiv 2k+1\pmod 7$,

$k\cdot 2^n+1\equiv 4k+1\pmod 5$,

$k\cdot 2^n+1\equiv 16k+1\pmod{17}$,

$k\cdot 2^n+1\equiv k+1\pmod{13}$,

$k\cdot 2^n+1\equiv 256k+1\pmod{241}$.

由中国剩余定理(注意上述每一个同余方程均有解),这样的 k 存在.

评注 这样的同余覆盖式不只一组,例如 $k\equiv 0\pmod 2$,$k\equiv 0\pmod 3$,$k\equiv 1\pmod 4$,$k\equiv 3\pmod 8$,$k\equiv 7\pmod{12}$,$k\equiv 23\pmod{24}$也是一组.

能力训练

1. 解同余方程组:(1) $\begin{cases} x\equiv 3\pmod 7 & ① \\ 6x\equiv 10\pmod 8 & ② \end{cases}$ (2) $\begin{cases} 3x\equiv 1\pmod{10} & ③ \\ 4x\equiv 7\pmod{15} & ④ \end{cases}$

2. 设 k 是给定的正整数,证明:一定存在 k 个相邻整数,其中任何一个数都能被大于 1 的立方数整除.

3. 设 k 是给定的正整数,$a_1,a_2,\cdots,a_k$ 是两两既约的正整数,证明:一定存在 k 个相邻整数,使第 j 个数被 a_j 整除($1\leqslant j\leqslant k$).

4. 给定任意正整数 n,存在 n 个相邻正整数,使得每个正整数的标准分解中,每个素数的幂次都小于或等于 1.

5. 设 n 为任意的正整数,证明:一定存在 n 个相邻整数,使其中任何一个都不是质数的幂.

6. 给定正整数 n,设 $f(n)$是使 $\sum_{k=1}^{f(n)}k$ 能被 n 整除的最小正整数. 证明:当且仅当 n 为 2 的幂时有 $f(n)=2n-1$.

7. 设 n,k 是给定的正整数,$n>0$,且 $k(n-1)$为偶数. 证明:存在 x,y,使得$(x,n)=(y,n)=1$,且 $x+y\equiv k\pmod n$.

8. 确定所有正整数 n,对它存在一个整数 m,使得 $2^{2^n}-1$ 是 m^2+9 的一个因数.

9. 设 $F(x)$为整系数多项式,已知对任何整数 n,$F(n)$都能被整数 $a_1,a_2,\cdots,a_m$ 之一

整除. 证明：可以从这些整数中选出一个数来，使得对任何 n，$F(n)$ 都能被它整除.

10. 任给一个正整数 n，存在一个整点，它与任意既约整点的距离大于 n（整点是指直角坐标为整数的点，既约整点则是坐标互素的点）.

§3.2 平方剩余

知识扫描

本节讨论平方剩余的一般理论和由此引出的"欧拉判别法". 在文末介绍 Legendre 符号.

平方剩余的出现源自解二次同余方程

$ax^2+bx+c\equiv 0(\bmod p)$， ①

p 为奇素数，$p\nmid a$.

我们在对①进行求解时，将它两边同乘以 $4a$，同加上 b^2，配方得：

$(2ax+b)^2\equiv b^2-4ac$，令 $y=2ax+b$，

所以 $y^2\equiv b^2-4ac(\bmod p)$，显然这个同余方程与①同时有解或无解. 这样我们只须讨论形如 $x^2\equiv d(\bmod p)$ 的同余方程，注意到当 $p\mid d$ 时，上式只有 $x\equiv 0(\bmod p)$ 这一解，所以，以后恒假定 $p\nmid d$，这样我们引进了平方剩余.

定义 1 设素数 $p>2$，d 是整数，$p\nmid d$，如果同余方程 $x^2\equiv d(\bmod p)$ 有解，则称 d 是模 p 的"二次剩余"（亦称平方剩余），若无解，则称 d 是模 p 的"非二次剩余".

例如，我们取 $p=5$，那么 $d\equiv 1,-1(\bmod 5)$ 是模 5 的二次剩余，取 $p=11$，那么 $d\equiv 1,3,4,5,9(\bmod 11)$ 是模 11 的二次剩余，一般地有以下结论：

定理 1 在模 p 的一个简化剩余系中，恰有 $\frac{p-1}{2}$ 个模 p 的二次剩余，$\frac{p-1}{2}$ 个模 p 的非二次剩余. 此外，若 d 是模 p 的二次剩余，则同余方程 $x^2\equiv d(\bmod p)$ 的解数为 2.

证 显然的，只要取模 p 的绝对最小简化剩余系：

$$-\frac{p-1}{2},-\frac{p-1}{2}+1,\cdots,-1,1,\cdots,\frac{p-1}{2}-1,\frac{p-1}{2} \qquad ②$$

来讨论，d 是模 p 的二次剩余当且仅当

$$d\equiv\left(-\frac{p-1}{2}\right)^2,\left(-\frac{p-1}{2}+1\right)^2,\cdots,(-1)^2,1^2,\cdots,\left(\frac{p-1}{2}-1\right)^2\text{或}\left(\frac{p-1}{2}\right)^2(\bmod p).$$

由于$(-j)^2\equiv j^2(\bmod p)$，所以 d 是模 p 的二次剩余当且仅当

$$d\equiv 1^2,2^2,\cdots,\left(\frac{p-1}{2}-1\right)^2,\left(\frac{p-1}{2}\right)^2(\bmod p). \qquad ③$$

上式给出了模 p 的全部二次剩余，共有$\frac{p-1}{2}$个，由于模 p 的简化剩余系有 $p-1$ 个数，所以另外的$\frac{p-1}{2}$个数必为模 p 的非二次剩余.

当 d 是模 p 的二次剩余时，注意到 $1\leqslant i<j\leqslant\frac{p-1}{2}$时，$i^2\not\equiv j^2(\bmod p)$，结合③知，必有唯一的 i，$1\leqslant i\leqslant\frac{p-1}{2}$，使 $x\equiv i(\bmod p)$是 $x^2\equiv d(\bmod p)$的解，进而推出在简化剩余系②中有且仅有 $x\equiv\pm i(\bmod p)$是 $x^2\equiv d(\bmod p)$的解，即同余方程 $x^2\equiv d(\bmod p)$的解数为 2，定理得证.

需要指明 x^2 恰能取$\left\{0,1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2\right\}$共$\frac{p-1}{2}+1$ 个值，即模 p 的完系中有$\frac{p+1}{2}$个二次剩余.

下面我们关心的是，对于什么样的 d，它是 $\bmod p$ 的二次剩余.

定理 2 （欧拉判别法）

设素数 $p>2$，$p\nmid d$，那么，d 是模 p 的二次剩余的充要条件是

$$d^{\frac{p-1}{2}}\equiv 1(\bmod p); \qquad ④$$

d 是模 p 的非二次剩余的充要条件是

$$d^{\frac{p-1}{2}}\equiv -1(\bmod p). \qquad ⑤$$

证 首先来证明对任一 d，$p\nmid d$，式④或⑤有且仅有一式成立，由费马小定理知 $d^{p-1}\equiv 1(\bmod p)$，因而有$\left(d^{\frac{p-1}{2}}-1\right)\left(d^{\frac{p-1}{2}}+1\right)\equiv 0(\bmod p)$，由于素数 $p>2$ 及$\left(d^{\frac{p-1}{2}}-1,d^{\frac{p-1}{2}}+1\right)|2$，所以推出④或⑤式有且仅有一式成立.

下面证明 d 是模 p 的二次剩余的充要条件是④成立，先证必要性.

若 d 是模 p 的二次剩余，则必有 x_0 使得

$d\equiv x_0^2(\bmod p)$，因而有 $x_0^{p-1}\equiv d^{\frac{p-1}{2}}(\bmod p)$.

由于 $p\nmid d$，所以 $p\nmid x_0$，由费马小定理知

$d^{\frac{p-1}{2}}\equiv x_0^{p-1}\equiv 1(\bmod p)$，必要性得证.

再证充分性，设④式成立，这时必有 $p\nmid d$. 考虑一次同余方程 $ax\equiv b(\bmod p)$，由 $p\nmid d$ 知对于由②式给出的模 p 的简化剩余系中的每个 j，当 $a=j$ 时，必有唯一的 $x=x_j$ 属于简化剩余系②使得 $ax\equiv b(\bmod p)$成立. 若 d 不是模 p 的二次剩余，必有 $j\neq x_j$，这样，简化

剩余系②中的 $p-1$ 个数即可按 j,x_j 一对，两两分完，因此有

$d^{\frac{p-1}{2}}\equiv(p-1)!\equiv-1(\bmod p)$（利用了 Wilson 定理）.

但这与④矛盾，所以必有某一 j_0，使 $j_0=x_{j_0}$，从而 d 是模 p 的二次剩余，充分性得证.

这样便完成了对欧拉判别式的证明.

例题分析

例 1 设 p 是奇质数，证明：-1 是模 p 的平方剩余的充要条件是 $p\equiv1(\bmod 4)$.

证明 由欧拉判别法，-1 是模 p 的平方剩余的充要条件为 $(-1)^{\frac{p-1}{2}}\equiv1(\bmod p)$，由 p 为奇质数，推出充要条件为 $\frac{p-1}{2}\equiv0(\bmod 2)$，即 $p\equiv1(\bmod 4)$，命题得证.

评注 从本例可以看出，欧拉判别法的实际作用并不在对具体的 p 进行判定，哪些是模 p 的二次剩余（实际上，当 p 不大时，直接利用 $d=1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2$ 得到二次剩余更快），而在于对属于某个特定剩余类或具有某些特定约束条件的广泛的 p 的二次剩余的性质进行讨论.

例 2 设 p 是满足 $p\equiv1(\bmod 4)$ 的奇质数，计算 $\sum\limits_{k=1}^{p-1}\left\{\frac{k^2}{p}\right\}$ 的值，其中 $\{x\}=x-[x]$，$[x]$ 为不超过 x 的最大整数.

解 由"例 1"知，$p\equiv1(\bmod 4)$ 时，-1 是模 p 的二次剩余，设 a 也是模 p 的二次剩余，由欧拉判别条件，$(-a)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}}\cdot a^{\frac{p-1}{2}}\equiv1(\bmod p)$. 即 $-a$ 也是模 p 的一个二次剩余，所以模 p 的二次剩余构成的集合 $\left\{1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2\right\}$ 在模 p 意义下即为

$\left\{a_1,p-a_1,a_2,p-a_2,\cdots,a_{\frac{p-1}{4}},p-a_{\frac{p-1}{4}}\right\}$，又当 $1\leqslant a_i,p-a_i<p$ 时，有

$$\left\{\frac{a_i}{p}\right\}+\left\{\frac{p-a_i}{p}\right\}=\frac{a_i}{p}+\frac{p-a_i}{p}=1,$$

所以 $\sum\limits_{k=1}^{p-1}\left\{\frac{k^2}{p}\right\}=2\sum\limits_{k=1}^{\frac{p-1}{2}}\left\{\frac{k^2}{p}\right\}=2\cdot\sum\limits_{i=1}^{\frac{p-1}{4}}\left(\left\{\frac{a_i}{p}\right\}+\left\{\frac{p-a_i}{p}\right\}\right)=\frac{p-1}{2}$.

下面是一个二次同余方程的例子.

例 3 求有序整数对 (a,b) 的个数，使得 $x^2+ax+b=167y$ 有整数解 (x,y)，其中 $1\leqslant a,b\leqslant2004$.

解 由定理 1 知，p 为奇质数时，S^2 模 p 恰能取 $\frac{p-1}{2}+1=\frac{p+1}{2}$ 个值（注意，这里 S 可取 0）.

这样，当存在 $x\in\mathbf{Z}$，使 $x^2+ax+b\equiv 0 \pmod{167}$ 时，则有整数解 (x,y). 上式两边同时乘以 4，配方，整理得：（这实际是解二次同余方程的步骤）

$a^2-4b\equiv(2x+a)^2 \pmod{167}$，

因此，a^2-4b 恰取模 167 的平方剩余（包含 0）共有 $\frac{167-1}{2}+1=84$ 个值（a 取 $0,1^2,2^2,\cdots,83^2$）.

又 $167\times 12=2004$，故每个 a 对应 84×12 个满足要求的 b，因此共有 $2004\times 12\times 84=2020032$ 个不同的有序整数对.

评注 解题时要注意题中的变量是在模 p 的简化剩余系中取值（有 $\frac{p-1}{2}$ 个二次剩余），还是在模 p 的完全剩余系中取值.

为了叙述的方便，我们引入 Legendre 符号.

定义 2 设素数 $p>2$，定义整变数 d 的函数

$$\left(\frac{d}{p}\right)=\begin{cases}1, & \text{当 } d \text{ 是模 } p \text{ 的二次剩余；}\\ -1, & \text{当 } d \text{ 是模 } p \text{ 的非二次剩余；}\\ 0, & \text{当 } p\mid d.\end{cases}$$

我们把 $\left(\frac{d}{p}\right)$ 称为 Legendre 符号，由本节定理 2，我们可以立即推出，Legendre 符号具有以下性质：

(ⅰ) $\left(\frac{d}{p}\right)=\left(\frac{p+d}{p}\right)$；

(ⅱ) $\left(\frac{d}{p}\right)\equiv d^{\frac{p-1}{2}} \pmod{p}$；

(ⅲ) $\left(\frac{1}{p}\right)=1$，$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$；

(ⅳ) $\left(\frac{dc}{p}\right)=\left(\frac{d}{p}\right)\cdot\left(\frac{c}{p}\right)$.

先看一个例子.

例 4 找出所有的质数 p，使得满足 $0\leqslant x,y\leqslant p$，且满足 $y^2\equiv x^3-x \pmod{p}$ 的整数对 (x,y) 恰有 p 对.

证明 记 $f(x)=x^3-x$，则 $f(x)$ 是奇函数，当 $p=2$ 时，$y^2\equiv f(x) \pmod{p}$ 恰有两解 $(0,0)$，$(1,0)$.

当 $p\equiv3(\bmod 4)$ 时，因为

$\left(\frac{-a}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{a}{p}\right)=-\left(\frac{a}{p}\right)$（利用了性质(iv)），

所以，$y^2\equiv f(x)$ 与 $y^2\equiv -f(x)\equiv f(-x)$ 一个有解，一个无解.

设 $x=2,3,\cdots,\frac{p-1}{2}$ 中，$y^2\equiv f(x)(\bmod p)$ 有 k 个解，则 $x=\frac{p+1}{2},\frac{p+3}{2},\cdots,p-2$ 中，$y^2\equiv f(x)(\bmod p)$ 有 $\frac{p-3}{2}-k$ 个有解.

所以，$x=2,3,\cdots,p-2$ 中，$y^2\equiv f(x)(\bmod p)$ 有 $\left(\frac{p-3}{2}-k\right)+k$ 个有解.

又对每个 $x=2,3,\cdots,p-2$，由 $y^2\equiv d(\bmod p)$ 必有两解，故 $x=2,3,\cdots,p-2$ 时，$y^2\equiv d(\bmod p)$ 有 $2\times\frac{p-3}{2}=p-3$ 个整数对 (x,y) 满足.

当 $x=0,1,p-1$ 时，$y^2\equiv f(x)\equiv0(\bmod p)$ 均只有一个整数对满足题意.

所以 $p\equiv3(\bmod 4)$ 时，同余方程有 p 组解.

当 $p\equiv1(\bmod 4)$ 时，

因为 $\left(\frac{-a}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{a}{p}\right)=\left(\frac{a}{p}\right)$，所以

$y^2\equiv f(x)$ 与 $y^2\equiv f(-x)$ 或同有两解或同无解.

设 $x=2,3,\cdots,\frac{p-1}{2}$ 中，$y^2\equiv f(x)(\bmod p)$ 有 k 个有解，则 $x=\frac{p+1}{2},\frac{p+3}{2},\cdots,p-2$ 中，$y^2\equiv f(x)$ 有 k 个有解.

类似于 $p\equiv3(\bmod 4)$ 的情形知，$x=2,3,\cdots,p-2$ 中，$y^2\equiv f(x)(\bmod p)$ 有 $2\times(k+k)$ 组 (x,y) 满足.

当 $x=0,1,p-1$ 时，$y^2\equiv f(x)\equiv0(\bmod p)$ 各有一组 (x,y) 满足要求.

所以共有 $4k+3$ 组解，而 $p\equiv1(\bmod 4)$，

故 $p\equiv1(\bmod 4)$ 时必不满足条件.

综上所述，$p=2$ 或 $p\equiv3(\bmod 4)$.

评注 从本例可以看出，用 Legendre 符号描述模的不同对二次剩余的影响较用欧拉判别法更方便，事实上，Legendre 符号的用武之处绝不仅仅如此，有兴趣的读者可参阅有关书籍.

最后再看一个例子，该例是二次剩余中的重要关系.

例 5 设 p 是素数且 $p\equiv1(\bmod 4)$，则 p 能写成两个平方数之和.

证明 因为 $p\equiv1(\bmod 4)$，故 $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=1$.

所以存在 $u\in\mathbf{Z}$，使得 $u^2+1\equiv 0(\bmod p)$.

故存在某个 $k(k\geqslant 1)$，满足 $u^2+1=kp$，即存在 $k(k\geqslant 1)$，使

$kp=x^2+y^2(x,y\in\mathbf{Z})$，

令 $r\equiv x(\bmod k)$，$s\equiv y(\bmod k)$，$-\frac{k}{2}<r,s\leqslant\frac{k}{2}$，

则 $r^2+s^2\equiv x^2+y^2\equiv 0(\bmod k)$，即存在 $k_1\in\mathbf{N}$，

使得 $r^2+s^2=k_1\cdot k$，

从而，$(r^2+s^2)(x^2+y^2)=k_1\cdot k\cdot kp=k_1k^2p$.

又 $(r^2+s^2)(x^2+y^2)=(rx+sy)^2+(ry-sx)^2$，

从而 $rx+sy\equiv x^2+y^2\equiv 0(\bmod k)$，

从而 $\left(\frac{rx+sy}{k}\right)^2+\left(\frac{ry-sx}{k}\right)^2=k_1p$，

由于 $rx+sy\equiv x^2+y^2\equiv 0(\bmod k)$，

$ry-sx\equiv xy-yx\equiv 0(\bmod k)$，

所以 $\frac{rx+sy}{k}$ 与 $\frac{ry-sx}{k}$ 均是整数，从而 k_1p 也可表示为两个数的平方和的形式.

因为 $k_1k=r^2+s^2\leqslant\left(\frac{k}{2}\right)^2+\left(\frac{k}{2}\right)^2=\frac{k^2}{2}$，则 $k_1\leqslant\frac{k}{2}<k$.

从而只要 $k\neq 1$，总存在一个 $k_1<k$，使得 k_1p 也可表示为两个数的平方和的形式.

因此，p 可表示为两个数的平方和(最后一步利用了递降的思想).

评注 由 $x^2+y^2\equiv 0,1,2(\bmod 4)$，这表明，若一个质数 p 能写成两个平方数和的形式，则它必然是 $4k+1$ 型的数.

能力训练

1. 设 p 是奇素数，且 $p\equiv 1(\bmod 4)$. 证明：

(1) $1,2,\cdots,\frac{p-1}{2}$ 中模 p 的二次剩余与二次非剩余的个数均为 $\frac{p-1}{4}$ 个；

(2) $1,2,\cdots,p-1$ 中有 $\frac{p-1}{4}$ 个偶数为模 p 的二次剩余，有 $\frac{p-1}{4}$ 个奇数为模 p 的二次非剩余；

(3) $1,2,\cdots,p-1$ 中全体模 p 的二次剩余之和为 $\frac{p(p-1)}{4}$.

2. 设 p 是奇素数. 证明：$1,2,\cdots,p-1$ 中全体模 p 的二次剩余之和 S 为 $\frac{p(p^2-1)}{24}-$

$p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{j^2}{p}\right]$.

3. 求所有的正整数 n，满足对所有的 n，都存在 m 使得 $2^n-1\mid m^2+9$.

4. 设 p 是一个 $4k+3$ 型的素数，求证：若 $p\mid a^2+b^2$，则 $p\mid a$ 且 $p\mid b$，其中 $a,b\in\mathbf{Z}$.

5. 设 k 是一个正整数. 证明：存在无穷多个形如 $n\cdot 2^k-7$ 的完全平方数，其中 n 为正整数.

6. 不存在整数 x,y 使得 $x^2+3xy-2y^2=122$.

7. 不存在一对正整数 x,y 满足 $3y^2=x^4+x$.

8. 证明：(1) 当素数 $p=4m+3$ 时，$\left(\frac{a}{p}\right)=1$ 时，$x_0=\pm a^{m+1}$ 是 $x^2\equiv a\pmod{p}$ 的解；(2) 当 $p=8m+5$，$\left(\frac{a}{p}\right)=1$ 时，求 $x^2\equiv a\pmod{p}$ 的解.

9. 证明：有无穷多个 $4k+1$ 型的素数.

10. 证明：有无穷多个 $8k+1$ 型的素数.

第四章 不定方程(组)

§4.1 公式法解不定方程

知识扫描

不定方程(组),是指未知数的个数多于方程(组)的个数,且未知数受到某些限制(如整数,正整数或有理数)的方程(组).

对于一个一般的不定方程(组),通常没有一个统一的解法,必须对不定方程的具体形式进行分析,确定解题方向.

下面讨论几种不定方程解题模式,我们称这些解法为公式法.

1. 一次不定方程

最简单的不定方程是整系数方程

$ax+by=c(ab\neq 0)$. ①

上述方程通常称为二元一次不定方程.

定理 1 二元一次不定方程①的系数都是整数,其有整数解的充要条件是$(a,b)|c$.

证 必要性 设 x_0, y_0 是①的解,则有 $ax_0+by_0=c$,设 $d=(a,b)$,则有 $d|ax_0$,$d|by_0$,所以 $d|c$.

充分性 设 $d=(a,b)$,且 $d|c$,有 $c=c_1d(c_1\in\mathbf{Z})$. 因 $d=(a,b)$,则存在 x_0,y_0 使得 $d=ax_0+by_0$,于是有 $c=c_1d=ac_1x_0+bc_1y_0$,所以 c_1x_0,c_1y_0 是①的整数解.

这样定理 1 得证,注意到①有解时,$(a,b)|c$ 则用(a,b)去除①的两端有

$a_1x+b_1y=c_1$, ②

此时,$(a_1,b_1)=1$,且②与①同解,因此,下面我们只用讨论$(a,b)=1$时,方程①的解.

定理 2 若$(a,b)=1$,且x_0,y_0为①之一解,则方程①的全部解为$x=x_0+bt$,$y=y_0-at(t\in\mathbf{Z})$

证 设x_0,y_0为①的解,则有

$ax_0+by_0=c$. ③

设x,y是①的任一解,①-③得

$a(x-x_0)+b(y-y_0)=0$.

因为$(a,b)=1$,于是有$b\mid(x-x_0)$,即$x-x_0=bt$,从而有$x=x_0+bt$,将此结果代入上式得$y=y_0-at$,即方程任一解都可表示为$x=x_0+bt$,$y=y_0-at(t\in\mathbf{Z})$.

反之,若x_0,y_0是①的解,则容易验证$x=x_0+bt$,$y=y_0-at$均是①的解,从而定理2得证.

依定理2,$x=x_0+bt$,$y=y_0-at$是方程①的解的一般形式,因此通常称为通解,相应地,x_0,y_0称为①的特解.

2. 勾股方程$x^2+y^2=z^2$

这是一个相当特殊的三元二次不定方程,它有鲜明的几何意义,并应用广泛.

这里只讨论勾股方程的正整数解,由方程不难看出,如果$(x,y)=d$,则$d^2\mid z^2$,从而$d\mid z$,这样可在勾股方程两边约去d^2,所以我们只须讨论满足$(x,y)=1$的解,此时易知x,y,z实际上两两互素,这种x,y,z两两互素的正整数解(x,y,z)称为勾股方程的本原解,也称为本原勾股数.

下面给出勾股方程的全部本原解.

定理 3 方程$x^2+y^2=z^2$满足$(x,y)=1$,$2\mid y$的全部正整数解(x,y,z)可表示为$x=a^2-b^2$,$y=2ab$,$z=a^2+b^2$,其中,a,b是满足$a>b>0$,a,b一奇一偶且$(a,b)=1$的任意整数.

证 设x,y,z是$x^2+y^2=z^2$的解,则由$2\mid y$,$(x,y)=1$不难看出x,z都是奇数,于是$\frac{z\pm x}{2}$是整数.

原方程变为$\left(\frac{y}{2}\right)^2=\frac{z+x}{2}\cdot\frac{z-x}{2}$, ④

而$\left(\frac{z+x}{2},\frac{z-x}{2}\right)=\left(\frac{z+x}{2},z\right)=\left(x,\frac{z-x}{2}\right)=1$(因$(x,z)=1$).

由于④的左边是完全平方数,故④右边互素的两个因子$\frac{z+x}{2}$和$\frac{z-x}{2}$也是完全平方

数，于是有 $a,b\in\mathbf{N}_+$ 且 $a>b$，使得 $\frac{z+x}{2}=a^2$，$\frac{z-x}{2}=b^2$（$(a,b)=1$），这样 $y=2ab$.

可解得 $x=a^2-b^2$，$y=2ab$，$z=a^2+b^2$，

由 $2\nmid x$ 知 a,b 一奇一偶.

3. 沛尔(Pell)方程

二元二次不定方程本质上归结为（双曲型）方程 $x^2-dy^2=c$ 的研究，其中 $d,c\in\mathbf{Z}$，$d>0$ 非平方数，而 $c\neq 0$.

此方程的一个特殊形式 $x^2-dy^2=1$ ⑤

最为重要，也最为基础，⑤称为沛尔方程.

能够证明（在此不予讨论）方程⑤一定有无穷多组正整数解，又设 (x_1,y_1) 是⑤的正整数解 (x,y) 中使 $x+y\sqrt{d}$ 最小的解，我们通常称 (x_1,y_1) 为最小解，则⑤的全部正整数解由

$$\begin{cases} x_n=\frac{1}{2}[(x_1+\sqrt{d}y_1)^n+(x_1-\sqrt{d}y_1)^n], \\ y_n=\frac{1}{2\sqrt{d}}[(x_1+\sqrt{d}y_1)^n-(x_1-\sqrt{d}y_1)^n] \end{cases} \quad ⑥$$

给出（$n=1,2,\cdots$）.

不难由⑥导出 x_n,y_n 满足的线性递推关系

$$\begin{cases} x_n=2x_1x_{n-1}-x_{n-2}, \\ y_n=2x_1y_{n-1}-y_{n-2}. \end{cases}$$

沛尔方程在数学竞赛中主要用于证明问题有无穷多个解，实际上对具体的 d，可用尝试法求出⑤的一组正整数解 (x_1,y_1)，无论 (x_1,y_1) 是否为最小解，由⑥均给出方程的无穷多组解.

例题分析

例 1 解不定方程 $143x-77y=187$.

解 因 $(143,77)=11$，且 $11\mid 187$，故原方程有整数解，且等价于 $13x-7y=17$. ①

在①两边模 7 得 $6x\equiv 3\pmod 7\Rightarrow 2x\equiv 1\pmod 7$，

故 $x\equiv 4\pmod 7$.

可取 $x=4$，代入①得 $y=5$.

于是得到①的特解 $x=4,y=5$.

由定理 2,原方程的一切整数解为$\begin{cases}x=4+7t,\\y=5+13t\end{cases}$ $(t\in\mathbf{Z})$.

例 2 求不定方程 $7x+19y=213$ 的正整数解.

解 由例 1 的方法求得原方程的一切整数解为$\begin{cases}x=25+19t,\\y=2-7t\end{cases}$ $(t\in\mathbf{Z})$.

令$\begin{cases}x=25+19t>0,\\y=2-7t>0,\end{cases}$

解得$-\frac{25}{19}<t<\frac{2}{7}$.

因为 $t\in\mathbf{Z}$,故 $t=0,-1$.

从而得原方程的正整数解为$\begin{cases}x=25,\\y=2,\end{cases}$$\begin{cases}x=6,\\y=9.\end{cases}$

例 3 求证:单位圆上有无穷多个有理点.

分析与证明 初看此题感觉无从下手,但细想后,联系到任何有理数都可表示成$\frac{p}{q}$ $(p,q\in\mathbf{Z},q\neq0)$的形式,可知此题实际上考的是变换了形式的勾股方程$\left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=1$,其正整数解为 $x=a^2-b^2$, $y=2ab$, $z=a^2+b^2$ $(a>b>0,a,b\in\mathbf{Z})$,这里只考虑了 $2\mid y$ 的情况,再结合方程知点$\left(\frac{a^2-b^2}{a^2+b^2},\frac{2ab}{a^2+b^2}\right)$是单位圆上的有理点,而 a,b 的取值有无穷多种,故单位圆上有无穷多个有理点.

例 4 求不定方程 $x^2+3y^2=z^2$,$(x,y)=1$ 的正整数解的通式.

解 $(x,z)=1$,x 是奇数,y,z 一奇一偶.

由 $3y^2=(z+x)(z-x)$,可令 $at=z+x$,$3bt=z-x$,$(a,b)=1$,

于是 $y^2=abt^2$,$a=u^2$,$b=v^2$,$(u,v)=1$.

又$(x,z)=1$ 及 $x=\frac{t(a-3b)}{2}$,$z=\frac{t(a+3b)}{2}$知只能是 $t=1$ 或 2.

若 $t=2$,则 $x=3u^2-2v^2$,$y=2uv$,$z=u^2+3v^2$.

若 $t=1$,则必须 $a\pm3b$ 是偶数,即 u,v 同为奇数.

对于 $3bt=z+x$,$at=z-x$ 的情况可作类似讨论.

解有两类:(1)$x=|u^2-3v^2|$,$y=2uv$,$z=u^2+3v^2$,u,v 一奇一偶,$(u,v)=1$;(2)$x=\frac{1}{2}|u^2-3v^2|$,$y=uv$,$z=\frac{1}{2}(u^2+3v^2)$,u,v 均为奇数,$(u,v)=1$.

例 5 在直角坐标平面上,以(199,0)为圆心,以 199 为半径的圆周上整点的个数为______.

解 设 $A(x,y)$ 为圆 O 上的任一整点，则其方程为 $(x-199)^2+y^2=199^2$.

显然，$(0,0)$，$(199,199)$，$(199,-199)$，$(398,0)$ 为方程的 4 组解，但当 $y\neq 0$、± 199 时，$(y,199)=1$（因 199 是质数），此时，$199,y,|199-x|$ 是一组勾股数，故 199 可表示为两个正整数的平方和，即 $199=m^2+n^2$.

因 $199=4\times 49+3$，可设 $m=2k,n=2l+1$. 则

$199=4k^2+4l^2+4l+1=4(k^2+l^2+l)+1$,

但这与 199 为 $4d+3$ 型质数矛盾，因而圆 O 上只有 4 个整点 $(0,0)$，$(199,199)$，$(398,0)$，$(199,-199)$.

例 6 求出方程 $x^2-7y^2=1$ 的所有正整数解.

解 先求最小解 (x_1,y_1)，令 $y=1,2,3,\cdots$.

$y=1$ 时，$1+7y^2=8$；$y=2$ 时，$1+7y^2=29$；$y=3$ 时，$1+7y^2=64=8^2$.

所以，$x^2-7y^2=1$ 的最小解为 $(8,3)$，于是

$$x_n=\frac{1}{2}[(x_1+\sqrt{d}y_1)^n+(x_1-\sqrt{d}y_1)^n]=\frac{1}{2}[(8+3\sqrt{7})^n+(8-3\sqrt{7})^n],$$

$$y_n=\frac{1}{2\sqrt{7}}[(8+3\sqrt{7})^n-(8-3\sqrt{7})^n]，其中 n=1,2,3,\cdots.$$

例 7 证明方程 $x^3+y^3+z^3+t^3=1999$ 有无穷多组整数解.

分析 本题是沛尔方程与方程解的表示知识的综合运用，令 $x=10-k,y=10+k,z=m,t=-1-m$，得 $(2m+1)^2-80k^2=1$，从而利用沛尔方程有通解的表达式.

解 注意到，$10^3+10^3+0^3+(-1)^3=1999$，我们寻找具有如下形式的满足方程的整数解：

$x=10-k,y=10+k,z=m,t=-1-m(k,m\in\mathbf{Z})$.

经代入原方程，化简可知 k,m 满足 $m(m+1)=20k^2$，

即 $(2m+1)^2-80k^2=1$.

这是一个沛尔方程，注意到 $m=4,k=1$ 是该沛尔方程的一个解，并且该方程的所有正整数解 (m_n,k_n) 满足：

$2m_n+1+k_n\sqrt{80}=(9+\sqrt{80})^n$,

这样的 (m_n,k_n) 有无穷多对，故原方程的整数解有无穷多组.

例 8 (1)证明存在无穷多个正整数 a，使 $a+1$ 和 $3a+1$ 都是平方数；

(2)若 $a_1<a_2<\cdots<a_n<\cdots$ 是(1)的全部正整数解组成的数列，证明：a_na_{n+1} 也是平方数.

解 (1)设 $a+1=y^2$，$3a+1=x^2$，则有不定方程

$x^2-3y^2=-2$, ①

易推得①的全部解(x_n, y_n)满足

$x_n+\sqrt{3}y_n=(2+\sqrt{3})^n(1+\sqrt{3}), n\in \mathbf{N}_+$. ②

这时 $a_n=y_n^2-1$，其中 $y_1=3, y_2=11, a_1=8, a_2=120$，等等.

(2)$a_na_{n+1}+1=(y_n^2-1)(y_{n+1}^2-1)+1=y_n^2y_{n+1}^2-y_n^2-y_{n+1}^2+2$.

为证它是平方数，须建立 y_{n+1} 与 y_n 间的关系，为此，由②有 $x_{n+1}+\sqrt{3}y_{n+1}=(2x_n+\sqrt{3}y_n)+\sqrt{3}(x_n+2y_n)$，

即$\begin{cases}x_{n+1}=2x_n+\sqrt{3}y_n,\\ y_{n+1}=x_n+2y_n.\end{cases}$

于是
$$\begin{aligned}a_na_{n+1}+1&=y_n^2y_{n+1}^2-y_n^2-x_n^2-4x_ny_n-4y_n^2+2\\&=(y_ny_{n+1}-2)^2+4y_ny_{n+1}-4-y_n^2-x_n^2-4x_ny_n-4y_n^2+2\\&=(y_ny_{n+1}-2)^2-(x_n^2-3y_n^2+2).\end{aligned}$$

但(x_n, y_n)是 $x^2-3y^2=-2$ 的解，故 $x_n^2-3y_n^2+2=0$，从而 a_na_{n+1}是平方数.

能力训练

1. 不定方程 $903x_1+731x_2=1106$ 有(　　)组正整数解.

A. 0　　B. 1　　C. 2　　D. 3

2. 不定方程 $96x_1+97x_2=1000$ 有(　　)组非负整数解.

A. 0　　B. 1　　C. 2　　D. 3

3. 设 $a,b,c\in \mathbf{N}_+$，$(a,b,c)=1$，又设$(a,b)=d$，则 $n>\dfrac{ab}{d}+cd-a-b-c$ 时，方程 $ax+by+cz=n$ 有非负整数解(x,y,z).

4. 求出 $x^2-2y^2=1$ 的所有正整数解.

5. 设 x,y,z 是 $x^2+y^2=z^2$ 的正整数解，证明：(1)$3|x$，$3|y$ 至少有一个成立；(2)$5|x$，$5|y$，$5|z$ 至少有一个成立.

6. 求 $x^4+y^2=z^2$ 满足$(x,y)=1$ 的全部正整数解.

7. 整数边直角三角形的内切圆半径长是整数.

8. 设 $k\in \mathbf{N}_+$，$k\geqslant 2$. 证明存在无穷多个整数 n，使得 $kn+1$ 及$(k+1)n+1$ 都是完全平方数.

9. 证明：有无穷多个正整数 n，使得$[\sqrt{2}n]$是完全平方数，($[x]$表示不超过 x 的最大整数).

§4.2 同余分析法解不定方程

知识扫描

解不定方程虽然没有固定套路，但大致思考方法还是有的，同余分析法就是一个很好的思考方法.

由于不定方程往往有太多的"不定性"，但方程的解是整数就让我们使同余分析法有了用武之地，在方程两边选取适当的模后，往往能找到方程的解应满足的某些必要条件，甚至推出方程无整数解，这样的论证灵活多变，在数学竞赛中尤为多见，本节将撷取一些例子来表现同余在这方面的运用.

例题分析

例 1 证明：不定方程 $x^2+y^2-8z^3=6$ 没有整数解.

证 模 2 知 x,y 奇偶性相同；模 4 可知 x,y 同为奇数，从而 $x^2\equiv1 \pmod 8$，$y^2\equiv1 \pmod 8$.

对方程两边模 8，有 $6\equiv x^2+y^2-8z^3\equiv2 \pmod 8$，矛盾. 所以原方程无整数解.

评注 此题取模方法还有很多，例如直接取模 8 亦可证明.

例 2 求所有正整数 $x>1,y>1,z>1$，使得 $1!+2!+\cdots+x!=y^z$. ①

解 关键一步是证明当 $x\geqslant8$ 时必有 $z=2$. 因为①的左边被 3 整除，故 $3\mid y^z$，从而 $3\mid y$，于是①的右边被 3^z 整除，另一方面，

$1!+2!+\cdots+8!=46233$

被 3^2 整除，但不被 3^3 整除；而对 $n\geqslant9$ 有 $3^3\mid n!$，所以，当 $x\geqslant8$ 时，①的左边被 3^2 整除，而不被 3^3 整除，从而①的右边也如此，即必须 $z=2$.

现在进一步证明，当 $x\geqslant8$ 时，方程①无解. ①两边模 5，当 $x\geqslant8$ 时有①左边 $\equiv1!+2!+3!+4!\equiv3 \pmod 5$；又已知 $z=2$，故①右边 $\equiv0,\pm1 \pmod 5$，从而上述断言成立.

最后，当 $x<8$ 时，通过验证可求得①的解是 $x=y=3$，$z=2$.

评注 此例中，通过比较某个素数在一个等式两边出现的幂次，以导出结果，同余的这种变形手法被称为比较素数幂法.

例 3 (2004 年巴尔干数学奥林匹克试题)已知 x，y 是质数，求不定方程 $x^y-y^x=xy^2-19$ 的解.

解 若 $x=y$，则显然无解.

由已知方程可得 $x^y\equiv-19(\bmod y)$，

由于 x，y 均为质数，且 $x\neq y$，所以 $(x,y)=1$.

由费尔马小定理，有 $x^{y-1}\equiv1(\bmod y)$，

于是，有 $x+19\equiv0(\bmod y)$，

同理 $19-y\equiv0(\bmod x)$，

因为 $x-y+19\equiv0(\bmod y)$，$x-y+19\equiv0(\bmod x)$，所以 $x-y+19\equiv0(\bmod xy)$.

易知 $x-y+19\neq0$，于是，有 $x+y+19>|x-y+19|\geqslant xy$，

即得 $(x-1)(y-1)<20$.

因此，$|x-y|<19$，$x-y+19\geqslant xy$，即 $(x+1)(y-1)\leqslant18$，

所以当 $x\geqslant5$ 时，$y=2$ 或 $y=3$.

但是 $x^2-2^x<0$，$x^3-3^x<0$，$xy^2-19>0$，矛盾.

从而 $x=4$. 容易验证，原不定方程的解为 $(2,3)$ 和 $(2,7)$.

评注 此题中的 x，y 是质数的条件让人联想到同余中的著名定理，从而以 x，y 为模直至解出本题，值得注意的是，此解答中还用到了不等式估计方法，此法在下一节会有介绍.

例 4 试证当 $2<n<11$ 时，不存在 n 个连续正整数，使得它们的平方和是完全平方数.

证 设 x 是非负整数，假设结论不成立，即存在 n 个连续正整数，使得它们的平方和是平方数 $y^2(y\in\mathbf{N}_+)$，设 $(x+1)^2+(x+2)^2+\cdots+(x+n)^2=y^2$.

即 $nx^2+n(n+1)x+\frac{1}{6}n(n+1)(2n+1)=y^2$，　　①

记 $A=\frac{1}{6}n(n+1)(2n+1)$，则 $y^2\equiv A(\bmod n)$，

当 $n=3,4,9$ 时，分别有 $A\equiv2(\bmod3)$，$A\equiv2(\bmod4)$，$A\equiv6(\bmod9)$，故 $n\neq3,4,9$.

当 $n=5,7$ 时，$n|A$，于是由①知 $n|y$，令 $y=nz$，代入①得

$x^2+(n+1)x+\frac{1}{6}(n+1)(2n+1)=nz^2$，

即 $\left(x+\frac{n+1}{2}\right)^2+\frac{1}{12}(n^2-1)=nz^2$，

以 $n=5,7$ 代入后将分别得到 $(x+3)^2\equiv-2(\bmod5)$，$(x+4)^2\equiv-4(\bmod7)$，但这是不可能的，故 $n\neq5,7$.

当 $n=6,8,10$ 时，由①得 $(n+1)(x^2+nx+\frac{1}{6}n(2n+1))=x^2+y^2$， ②

若 $n=6$，则由②知 $x^2+y^2\equiv0\pmod 7$，

由于 $x^2\equiv0,1,2,4\pmod 7$，因此需使 $x^2+y^2\equiv0\pmod 7$ 成立，

只能 $x\equiv0, y\equiv0\pmod 7$，于是由②知有 $7^2\mid\frac{1}{6}n(n+1)(2n+1)=7\times13$，矛盾.

故 $n\neq6$，同理可证 $n\neq10$.

若 $n=8$，则由②可得 $x^2+y^2=9x^2+8\times9x+\frac{1}{6}\times8\times9\times17\equiv204\equiv6\pmod 9$，

而 $x^2\equiv0,1,4,7\pmod 9$，故此式不成立，$n\neq8$.

综上所述，命题得证.

例 5 （2003 年英国数学奥林匹克）

已知 $34!=295232799cd96041408476186096435ab000000$，求数字 a,b,c,d 的值.

解 由于 $34!=k\times11^3\times7^4\times5^7\times3^{15}\times2^{32}=k\times11^3\times7^4\times3^{15}\times2^{25}\times10^7$，

所以 $b=0$，$a\neq0$.

考虑去掉最后面的 7 个零时的情形，知该数可以被 2^{25} 整除，也可以被 8 整除，即最后三位 $\overline{35a}$ 可以被 8 整除（因为 1000 可以被 8 整除），因此 $a=2$.

由于 34! 可以被 9 整除，所以，其各位数字之和也可以被 9 整除，于是，$141+c+d\equiv0\pmod 9$，即 $c+d\equiv3\pmod 9$.

而 34! 还可以被 11 整除，所以，奇数位与偶数位上数字之和的差可以被 11 整除，于是，$80+d\equiv61+c\pmod{11}$，即 $8+d\equiv c\pmod{11}$，

当 $c+d=3$，$8+d=c$ 时，无解；

当 $c+d=12$，$8+d=c$ 时，无解；

当 $c+d=12$，$d=c+3$ 时，无解；

当 $c+d=3$，$d=c+3$ 时，得 $c=0$，$d=3$.

综上所述，$a=2$，$b=0$，$c=0$，$d=3$.

评注 此题的条件让人望而生畏，但仔细思考就会联想到某些数可整除的数所具有的性质，进而解出此题.

例 6 证明：不定方程 $8^x+15^y=17^z$ ①

的全部正整数解是 $x=y=z=2$.

证 我们先用同余证明：y 和 z 都是偶数.

方程①模 4，得到 $(-1)^y\equiv1\pmod 4$，

从而 y 是偶数，将方程①模 16，得到 $8^x+(-1)^y\equiv1\pmod{16}$，

即 $8^x\equiv0\pmod{16}$，故 $x\geqslant2$.

注意 $17^2 \equiv 1, 15^2 \equiv 1 \pmod{32}$，故若 z 是奇数，则由 $2 \mid y$ 及 $x \geqslant 2$，可从①得出 $1 \equiv 17 \pmod{32}$。

这不可能，所以 z 必为一个偶数.

设 $y=2y_1, z=2z_1$，则方程①可分解为

$$(17^{z_1}-15^{y_1})(17^{z_1}+15^{y_1})=8^x, \quad ②$$

易知②中左边两个因数的最大公约数为 2，而②的右边是 2 的幂，故必须有

$$\begin{cases} 17^{z_1}-15^{y_1}=2 & ③ \\ 17^{z_1}+15^{y_1}=2^{3x-1} & ④ \end{cases}$$

将③模 32 可知 z_1 与 y_1 必须都是奇数(否则，③的左边 $\equiv 0, -14, 16 \pmod{32}$)，将③、④相加得 $17^{z_1}=1+2^{3x-2}$， ⑤

若 $x \geqslant 3$，则⑤的右边 $\equiv 1 \pmod{32}$；而因 z_1 是奇数，故⑤左边 $\equiv 17 \pmod{32}$，这不可能，故必有 $x=2$. 由此及⑤得 $z_1=1$，即 $z=2$，进而易知 $y_1=1$，即 $y=2$. 因此 $x=y=z=2$.

评注 这一解法是同余结合分解方法的典型的例子.

例 7 (2003 年英国数学奥林匹克试题)求所有正整数 a, b, c 满足 $(a!)\cdot(b!)=a!+b!+c!$.

解 不失一般性，假设 $a \geqslant b$，则原方程化为 $a!=\frac{a!}{b!}+1+\frac{c!}{b!}$.

由于上式中有三项 $a!, \frac{a!}{b!}, 1$ 是整数，所以 $c \geqslant b$.

又因为右边的每一项都是正整数，则其和至少是 3. 因此，$a \geqslant 3$，且 $a!$ 是偶数.

于是，$\frac{a!}{b!}$ 和 $\frac{c!}{b!}$ 中有且仅有一项是奇数.

(1) 假设 $\frac{a!}{b!}$ 是奇数，则要么 $a=b$，要么 $\frac{a!}{b!}=b+1$ 且 $b+1$ 是奇数，$a=b+1$.

(i) 若 $a=b$，则 $a!=2+\frac{c!}{a!}$，

当 $a=3$ 时，有 $b=3, c=4$，

当 $a>3$ 时，由于 $a!-2 \equiv -2 \pmod{3}$，所以

$c=a+1$ 或 $a+2$ (否则 $\frac{c!}{a!} \equiv 0 \pmod{3}$).

$\frac{c!}{a!}=a+1$ 或 $(a+1)(a+2)$，

$$a!=(a+3) \text{ 或 } (a+1)(a+2)+2, \quad ①$$

当 $a=4$ 或 5 时，不满足①.

当 $a \geqslant 6$ 时，明显①左边大于右边，此时原方程无解.

(ⅱ)若 $a=b+1$，其中 b 是偶数，

则原方程化为 $(b+1)!=b+2+\frac{c!}{b!}$，

两边模 $b+1$ 得 $\frac{c!}{b!}\equiv -1(\bmod (b+1))$.

又知 $\frac{a!}{b!}$ 为奇数时，$\frac{c!}{b!}$ 为偶数，故 $c>b$.

于是 $\frac{c!}{b!}\equiv 0(\bmod (b+1))$，矛盾.

(2)假设 $\frac{a!}{b!}$ 是偶数，$\frac{c!}{b!}$ 是奇数，则 $c=b$ 或 $c=b+1$（b 为偶数）.

(ⅰ)若 $c=b$，则方程化为 $(a!)\cdot(b!)=(a!)+2\times(b!)$，

所以 $\frac{a!}{b!}(b!-1)=2$. 故 $\frac{a!}{b!}=2, b!-1=1$.

于是 $b=2, a!=4$，矛盾.

(ⅱ)若 $c=b+1$，则方程化为 $(a!)(b!)=(a!)+(b+2)(b!)$.

所以 $(a!)(b!-1)=(b+2)(b!)$.

由于 $(b!, b!-1)=1$，因此 $(b!-1)\mid b+2$.

因为 b 是偶数，所以，$b=2, a!=8$，不可能.

综上所述，原方程有唯一解 $a=3, b=3, c=4$.

评注 此题的关键在于奇偶性的分类讨论，而奇偶性的分析实质上是模为 2 的同余分析.

能力训练

1.（2004 年韩国数学奥林匹克）证明：不存在一对正整数 x,y 满足 $3y^2=x^4+x$.

2. 若 $n\equiv 4(\bmod 9)$，证明不定方程 $x^3+y^3+z^3=n$ 没有整数解 (x,y,z).

3. 证明：不定方程 $(x+2)^{2m}=x^n+2$ 没有正整数解.

4. 求所有正整数 m,n，使得 $|12^m-5^n|=7$.

5. 证明：不定方程 $5^x-3^y=2$ 仅有正整数解 $x=y=1$.

6. 试确定使 ab^2+b+7 整除 a^2b+a+b 的全部正整数对 (a,b).

7. 求出所有正整数 m,n，使 2^m+3^n 是完全平方数.

8. 证明：不定方程 $(x+1)^y-x^z=1$，$x,y,z>1$ 仅有一组正整数解 $x=2,y=2,z=3$.

9. 证明：方程 $y^2=x^3+7$ 没有整数解.

10. 求方程 $3^x=2^x y+1$ 的正整数解.

11.（2005 年美国数学奥林匹克试题）证明：方程组 $\begin{cases}x^6+x^3+x^3y+y=147^{157}\\x^3+x^3y+y^2+y+z^9=157^{147}\end{cases}$ 没有整数解 x,y,z.

§4.3 各种方法的综合运用

知识扫描

除了同余分析法外，处理不定方程的技巧还有很多，例如分解法、不等式分析法等，下面我们将介绍几种方法用处.

1. 分解法

将方程的一边化为常数，作质因数分解，另一边含未知数的代数式也作因式分解，考查各个因式的取值情况，再配对求解.

其实，在前一节的解题的各种解答中，都很自然地用到了分解法，因为此法就是对方程的解是整数的最好的体现.

2. 不等式分析法

不等式分析法是指通过对所考察的量的放缩得到未知数取值条件的不等式，解这些不等式就得到未知数取值的范围，从而达到求解目的的方法.

3. 构造法

对于某些存在性命题，常采用构造法，构造一些数学模型来解决.

4. 换元法

若能判明不定方程的未知数之间有倍数关系，则常使用换元法消去未知数或倍数，使方程简化.

5. 无穷递降法

非常重要的一种方法，将在第六章详细介绍.

例题分析

例 1 找出所有正整数组(x,y,z)，使得y是质数，y和3均不被z整除，且$x^3-y^3=z^2$.

分析 将$x^3-y^3=z^2$因式分解，利用y为质数得到，$x-y=m^2$，$x^2+xy+y^2=n^2$，$z=mn$，从而有$3y^2=(2n+2x+y)(2n-2-y)$，再利用y为质数，分情况讨论即可.

解 由题意知$(x-y)[(x-y)^2+3xy]=z^2$， ①

因为y是质数，且y和3均不被z整除，所以$(x,y)=1$，$(x-y,3)=1$.

于是$(x^2+y^2+xy,x-y)=(3xy,x-y)=1$. ②

由①，②两式得

$x-y=m^2$，$x^2+xy+y^2=n^2$，$z=mn(m,n\in\mathbf{N}_+)$，

于是$3y^2=4n^2-(2x+y)^2=(2n+2x+y)(2n-2x-y)$.

又y为质数，且$2n-2x-y<2n+2x+y$.

则有下列3种情况：

(1)$2n-2x-y=y$，$2n+2x+y=3y$，得$x=0$，舍去.

(2)$2n-2x-y=3$，$2n+2x+y=y^2$，则$y^2-3=4x+2y=4m^2+6y$，

所以$(y-3)^2-4m^2=12$，解得$y=7$，$m=1$.

故$x=8$，$y=7$，$z=13$.

(3)$2n-2x-y=1$，$2n+2x+y=3y^2$，则$3y^2-1=4x+2y=2(2m^2+3y)$，

即$3y^2-6y-4m^2-1=0$，于是$m^2+1\equiv0\pmod 3$.

但$m^2\equiv0$或$1\pmod 3$，矛盾.

综上所述满足条件的正整数组是唯一的，即$(8,7,13)$.

例 2 (2004年中国台湾数学奥林匹克试题)求所有正整数对(a,b)，满足$\sqrt{\frac{ab}{2b^2-a}}=\frac{a+2b}{4b}$.

解 将$\sqrt{\frac{ab}{2b^2-a}}=\frac{a+2b}{4b}$两边平方并化简，得

$a(a^2+4ab+4b^2)=2b^2(a^2-4ab+4b^2)$，

即$a(a+2b)^2=2b^2(a-2b)^2$， ①

因上式左边为偶数，故令$a=2t^2$，$t\in\mathbf{N}_+$，代入①并化简得

$t^2(2t^2+2b)^2=b^2(2t^2-2b)^2$，

即$t(t^2+b)=b|t^2-b|$， ②

所以，$t=\frac{b|t^2-b|}{t^2+b}$.

当 $b<t^2$ 时，由式②得 $b^2+(t-t^2)b+t^3=0$，

解得 $b=\frac{t}{2}(t-1\pm\sqrt{t^2-6t+1})$.

设 $\sqrt{t^2-6t+1}=s$，且 $s\in\mathbf{N}_+$，

平方并化简整理得 $(t+s-3)(t-s-3)=8$.

由此得出唯一一组正整数解 $\begin{cases}t=6,\\s=1.\end{cases}$

故 $\begin{cases}a=72,\\b=18.\end{cases}$ 或 $\begin{cases}a=72,\\b=12.\end{cases}$

当 $b\geqslant t^2$ 时，类似的可得 $t=0$，矛盾.

综上所述，只有两组正整数解 $\begin{cases}a=72,\\b=18;\end{cases}$ $\begin{cases}a=72,\\b=12.\end{cases}$

例 3 (2004 年希腊数学奥林匹克试题)证明：不存在正整数 $x_1,x_2,\cdots,x_m,m\geqslant2$，使得 $x_1<x_2<\cdots<x_m$，且 $\frac{1}{x_1^3}+\frac{1}{x_2^3}+\cdots+\frac{1}{x_m^3}=1$.

证 如果 $x_1=1$，则 $\frac{1}{x_1^3}=1$，且 $\frac{1}{x_1^3}+\frac{1}{x_2^3}+\cdots+\frac{1}{x_m^3}>1$，矛盾.

如果 $x_1\geqslant2$，则 $x_i\geqslant i+1$，$i=1,2,\cdots,m$.

注意到 $\frac{1}{x_i^3}\leqslant\frac{1}{(i+1)^3}<\frac{1}{(i+1)^2}<\frac{1}{i(i+1)}=\frac{1}{i}-\frac{1}{i+1}$，

所以 $\sum_{i=1}^{m}\frac{1}{x_i^3}<\left(1-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\cdots+\left(\frac{1}{m}-\frac{1}{m+1}\right)=1-\frac{1}{m+1}<1$，矛盾.

因此不存在满足条件的正整数.

例 4 (2004 年斯洛文尼亚数学奥林匹克选拔赛试题)试求表达式 $\left(b-\frac{1}{a}\right)\left(c-\frac{1}{b}\right)\left(a-\frac{1}{c}\right)$ 的值为整数的所有正整数 a,b,c.

解 由于问题的对称性，我们考虑 $a\leqslant b\leqslant c$ 的情形，注意到表达式的值是整数，则有 $abc\mid[(ab-1)(bc-1)(ca-1)]$，

即 $abc\mid(a^2b^2c^2-a^2bc-ab^2c-abc^2+ab+bc+ac-1)$，

则 $abc\mid(ab+bc+ca-1)$，

故 $abc\leqslant ab+bc+ca-1<ab+bc+ca\leqslant c(a+a+b)$，

从而 $ab<2a+b\leqslant3b$. 于是 $a\leqslant3$.

如果 $a=1$，则 $bc\mid(b+c-1)$，且 $bc-b-c+1=(b-1)(c-1)\leqslant0$，

这必然导致 $b=1$(或 $c=1$,但 $b\leqslant c$).

如果 $a=2$,则 $2bc\mid(bc+2b+2c-1)$.

于是 $bc\leqslant 2b+2c-1<2b+2c\leqslant 4c$,从而 $b<4$.

若取 $b=2$,则有 $4c\mid 4c+3$.

从而 $4c\mid 3$,这是不可能的.

若取 $b=3$,则有 $6c\mid 5c+5$,从而 $6c\leqslant 5c+5\Rightarrow c\leqslant 5$.

通过检验所有情形,可知只有 $c=5$ 是可能的.

因此,所有的解(按 $a\leqslant b\leqslant c$)是 $(1,1,c)$ 和 $(2,3,5)$,其中 c 是任意的,由于问题的对称性,a,b,c 的顺序是任意的,故所求解为

$(1,1,c),(1,c,1),(c,1,1),(2,3,5),(2,5,3),(3,2,5),(3,5,2),(5,2,3),(5,3,2)$.

例 5 (2004 年白俄罗斯数学奥林匹克试题)正整数 a,b,c 满足等式 $c(ac+1)^2=(5c+2b)(2c+b)$. ①

(1)证明:若 c 为奇数,则 c 为完全平方数;

(2)对某个 a,b 是否存在偶数 c 满足①;

(3)证明:式①有无穷多组正整数解 (a,b,c).

解 先解(2).

(2)假设 c 为偶数,记 $c=2c_1$.则已知等式可写为 $c_1(2ac_1+1)^2=(5c_1+b)(4c_1+b)$.

设 $d=(c_1,b)$,则 $c_1=dc_0$,$b=db_0$,其中 $(c_0,b_0)=1$.

于是,有 $c_0(2adc_0+1)^2=d(5c_0+b_0)(4c_0+b_0)$.

显然,$(c_0,5c_0+b_0)=(c_0,4c_0+b_0)=(d,(2adc_0+1)^2)=1$.

因此,$c_0=d$.从而,$(2ad^2+1)^2=(5d+b_0)(4d+b_0)$.

注意到

$$\begin{aligned}(5c_0+b_0,4c_0+b_0)&=(5c_0+b_0-4c_0-b_0,4c_0+b_0)\\&=(c_0,4c_0+b_0)=(c_0,4c_0+b_0-4c_0)\\&=(c_0,b_0)=1,\end{aligned}$$

所以,$5d+b_0=m^2$,$4d+b_0=n^2$,$2ad^2+1=mn$,$m,n\in\mathbf{N}_+$.

于是,$d=m^2-n^2$(显然 $m>n$),则

$mn=1+2ad^2=1+2a(m-n)^2(m+n)^2$

$\geqslant 1+2a(m+n)^2\geqslant 1+2a\cdot 4mn\geqslant 1+8mn$,矛盾.

因此 c 是奇数,即对某个 a,b 不存在偶数 c 满足式①.

(1)类似(2),设 $(c,b)=d$,$c=dc_0$,$b=db_0$,且 $(c_0,b_0)=1$.

则已知等式改写为 $c_0(adc_0+1)^2=d(5c_0+2b_0)(2c_0+b_0)$.

注意到 $(c_0,5c_0+2b_0)=(c_0,2c_0+b_0)=(d,(adc_0+1)^2)=1$.

因此,$c_0=d$,从而,$c=dc_0=d^2$.

(3)令 $c=1$，只需证明方程 $(a+1)^2=(5+2b)(2+b)$ 有无穷多组整数解 (a,b).

事实上，设 $5+2b=m^2$，$2+b=n^2$，则 $a=mn-1$.

从而只需证明：存在无穷多组 $m,n\in\mathbf{N}_+$ 满足 $5+2b=m^2$，$2+b=n^2$，即 $m^2-2n^2=1$.

这是一个沛尔方程，它有无穷多组解，从而原命题成立.

例 6 试求所有正整数 n，使方程 $x^3+y^3+z^3=nx^2\cdot y^2\cdot z^2$ 有正整数解.

解 不妨设 $x\leqslant y\leqslant z$，显然 $z^2\mid x^3+y^3$，故 $z^2\leqslant x^3+y^3$，但 $x^3\leqslant xz^2$，$y^3\leqslant yz^2$.

将 $x^3+y^3+z^3=nx^2y^2z^2$ 变形有

$$z=nx^2y^2-\frac{x^3+y^3}{z^2}\geqslant nx^2y^2-(x+y),$$

于是 $x^3+y^3\geqslant z^2\geqslant[nx^2y^2-(x+y)]^2$，$n^2x^4y^4<2nx^2y^2(x+y)+x^3+y^3$，

$$nxy<2\left(\frac{1}{x}+\frac{1}{y}\right)+\frac{1}{nx^3}+\frac{1}{ny^3}. \qquad ①$$

易知 $x=1$，否则若 $x\geqslant 2$，而 $y\geqslant 2$，则①式左边不小于 4，而右边显然小于 3，①将不成立.

由 $x=1$，得 $ny<2+\dfrac{2}{y}+\dfrac{1}{n}+\dfrac{1}{ny^3}$.

上式只能在 $y\leqslant 3$ 时才能成立，但 $z^2\mid(1+y^3)$. 由此只能是 $y=1,2$（当 $y=3$ 时，$z^2\mid 28$，$z^2=1,4$ 与 $z\geqslant y$ 矛盾），相应地，$z=1,3$.

综合上述讨论，只能有 $x=y=1$ 或 $x=1,y=2,z=3$，因而 n 只能取 3，1.

评注 此例把等式变形为不等式①后，由于左边变量 x,y 的指数是正数，右边的指数是负数，因而当 x,y 增大时，左边的值增大，而右边的值减小，这样，x,y 就有一个上限，当 x,y 大于此上限时，①不再成立. 据此，并利用 x,y 是整数的要求，我们就只有对有限几个 x,y 值进行验算，即可获解.

例 7 试证：如果正整数 n 使方程 $x^3-3xy^2+y^3=n$ 有一组整数解 (x,y)，那么这个方程至少有三组整数解.

分析 此题是个存在性命题，采用构造法，即若 (x,y) 为已知解，利用它至少可构造出其他不同的两组解来.

解 因为 (x,y) 为一组整数解，则

$$\begin{aligned}(y-x)^3&=y^3-3xy^2+3x^2y-x^3\\&=y^3-3xy^2+x^3+3x^2(y-x)+x^3\\&=n+3x^2(y-x)+x^3,\end{aligned}$$

所以，$(y-x)^3-3(y-x)(-x)^2-x^3=n$.

即 $(y-x)^3-3(y-x)(-x)^2+(-x)^3=n$，

因此，$(y-x,-x)$ 也是原方程的一组解.

记 $u=y-x, v=-x$，则 (u,v) 也是原方程的一组解，同样，可令 $u'=v-u, v'=-u$，则 $u'=-y, v'=x-y$，于是由上知 (u',v') 也是原方程的一组解. 下面证明 (x,y)，$(y-x,-x)$，$(-y,x-y)$ 是原方程的 3 组不同的解.

若 $(x,y)=(y-x,-x)$，得 $x=0, y=0$ 代人原方程得 $n=0$，与 n 为正整数，矛盾.

同样可证 $(x,y)\neq(-y,x-y)$，$(-y,x-y)\neq(y-x,-x)$. 这就证明了原方程若有整数解，则至少有三组整数解.

例 8 （第 43 届 IMO 预选题）是否存在正整数 m，使得方程 $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{abc}=\frac{m}{a+b+c}$ 有无穷多组正整数解.

解 存在.

如果 $a=b=c=1$，则 $m=12$，令

$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{abc}-\frac{12}{a+b+c}=\frac{p(a,b,c)}{abc(a+b+c)}$，

其中 $p(a,b,c)=a^2(b+c)+b^2(c+a)+c^2(a+b)+a+b+c-9abc$.

假设 (x,a,b) 是满足 $p(x,a,b)=0$ 的一组解，且 $x\leqslant a\leqslant b$，由于 $p(x,a,b)=0$ 是关于 x 的二次方程，所以，$y=\frac{ab+1}{x}>b$ 是其另外一个解.

设 $a_0=a_1=a_2=1$，定义 $a_{n+2}=\frac{a_na_{n+1}+1}{a_{n-1}}(n\geqslant 1)$.

我们证明下列结论：

(1) $a_{n-1}\mid(a_na_{n+1}+1)$；

(2) $a_n\mid(a_{n-1}+a_{n+1})$；

(3) $a_{n+1}\mid(a_{n-1}a_n+1)$.

其中 a_{n-1}, a_n, a_{n+1} 均为正整数.

当 $n=1$ 时，以上 3 个结论显然成立.

假设 $n=k$ 时以上 3 个结论也成立.

由(1)得 $a_{k-1}\mid(a_ka_{k+1}+1)$，即 a_{k-1} 与 a_k 互素，

且 $a_{k-1}\mid[(a_ka_{k-1}+1)a_{k+1}+a_{k-1}]$；

由(2)得 $a_k\mid(a_{k-1}+a_{k+1})$，且 $a_k\mid(a_ka_{k+1}^2+a_{k+1}+a_{k-1})$，

所以 $a_ka_{k-1}\mid(a_ka_{k+1}^2+a_{k+1}+a_{k-1})$，

即 $a_k\left|\left(a_{k+1}\frac{a_ka_{k-1}+1}{a_{k-1}}+1\right)\right.\Rightarrow a_k\mid(a_{k+1}a_{k+2}+1)$.

于是当 $n=k+1$ 时(1)也成立.

同理，由于 a_{k-1} 与 a_{k+1} 也互素，且 $a_{k-1}\mid(a_ka_{k+1}+1+a_ka_{k-1})$，

由(3)得 $a_{k+1}|(a_{k-1}a_k+1)$，且 $a_{k+1}|(a_{k-1}a_k+1+a_ka_{k+1})$，

所以 $a_{k-1}a_{k+1}|[a_k(a_{k-1}+a_k)+1]$，

即 $a_{k+1}\left|\left(a_k+\frac{a_ka_{k-1}+1}{a_{k-1}}\right)\right.\Rightarrow a_{k+1}|(a_k+a_{k+2})$，

于是，当 $n=k+1$ 时，(2)也成立.

由 a_{k+2} 的定义及(1)知 a_{k+2} 是整数，且 $a_{k+2}|(a_ka_{k+1}+1)$，

于是，当 $n=k+1$ 时(3)也成立.

从而可得数列 $\{a_n\}$，当 $n\geqslant 2$ 时严格递增，且 $p(a_n,a_{n+1},a_{n+2})=0$，即 (a_n,a_{n+1},a_{n+2}) 是原方程的解，$\{a_n\}=\{1,1,1,2,3,7,11,26,41,97,153,\cdots\}$.

能力训练

1. 求不定方程 $x^4+y^4+z^4=2x^2y^2+2y^2z^2+2z^2x^2+24$ 的全部整数解.

2. 求方程 $x(x+1)=y^7$ 的正整数解.

3. 找出满足 $\frac{1}{2}(a+b)(b+c)(c+a)+(a+b+c)^3=1-abc$ 的全部整数 a,b,c，并做必要的证明.

4. (2003 年土耳其数学奥林匹克)求方程 $x^m=2^{2n+1}+2^n+1$ 的三元正整数解 (x,m,n).

5. (2004 年澳大利亚数学奥林匹克)求使 $(a^3+b)(a+b^3)=(a+b)^4$ 成立的所有整数对 (a,b).

6. (2003 年芬兰高中数学竞赛)求满足 $(n+1)^k-1=n!$ 的所有正整数对 (n,k).

7. (2003 年俄罗斯数学奥林匹克)求所有质数 p，使得 $p^x=y^3+1$ 成立，其中 x,y 是正整数.

8. (2003 年北欧数学竞赛)求所有的三元整数组 (x,y,z)，使得 $x^3+y^3+z^3-3xyz=2003$.

9. (2004 年斯洛文尼亚数学奥林匹克)求方程 $a^6=ab+2$ 的全部整数解.

10. (2005 年越南数学奥林匹克)求所有满足关系式 $\frac{x!+y!}{n!}=3^n$ 的自然数组 (x,y,n)(约定 $0!=1$).

第五章　高斯函数

§5.1　高斯函数的定义与基本性质

知识扫描

(一)定义

设 x 是实数，不超过 x 的最大整数记为 $[x]$，称 $[x]$ 为高斯函数. 将 $[x]$ 叫做 x 的整数部分，$x-[x]$ 叫做 x 的小数部分，记为 $\{x\}$.

(二)基本性质

(1) $x=[x]+\{x\}$，$0\leqslant\{x\}<1$；

(2) $x-1<[x]\leqslant x<[x]+1$；

(3) $[n+x]=n+[x]$，$\{n+x\}=\{x\}$，$n\in\mathbf{Z}$；

(4) 若 $x\leqslant y$，则 $[x]\leqslant[y]$；

(5) 当 $x\in\mathbf{Z}$ 时，$[-x]=-[x]$，当 $x\notin\mathbf{Z}$ 时，$[-x]=-[x]-1$；

(6) 若 $n\in\mathbf{N}$，$x\in\mathbf{R}$，则 $\left[\frac{x}{n}\right]=\left[\frac{[x]}{n}\right]$；

(7) $[x]+[y]\leqslant[x+y]$.

(三)高斯函数的图象

对于函数 $y=[x]$，其定义域是全体实数，值域是整数集 $\mathbf{Z}$. 对任意整数 n，函数 $y=[x]$ 在 $[n,n+1)$ 上的图形是一段平行于 x 轴的线段(不含右端点)，因此可以说高斯函数

的图象是成阶梯状分布的，且在每个整点上都有一个跳跃型的间断.

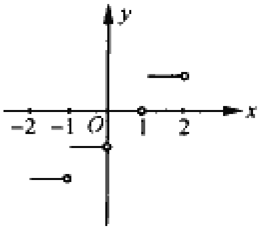


图 5-1

例题分析

例 1 计算和式 $S=\sum_{n=1}^{509}\left[\frac{511n}{509}\right]$的值.

分析 首先应将$\frac{511}{509}$化为带分数的形式，如此一来便可将$\frac{511n}{509}$化为一个整数与另一部分的和.

解 $S=\sum_{n=1}^{509}\left[n+\frac{2n}{509}\right]=\sum_{n=1}^{509}\left(n+\left[\frac{2n}{509}\right]\right)=\sum_{n=1}^{509}n+\sum_{n=1}^{509}\left[\frac{2n}{509}\right]$.

当 $1\leqslant n\leqslant 254$ 时，$2n<509$，$\left[\frac{2n}{509}\right]=0$；

当 $255\leqslant n\leqslant 508$ 时，$509<2n<509\times 2$，$\left[\frac{2n}{509}\right]=1$；

当 $n=509$ 时，$\left[\frac{2n}{509}\right]=2$.

故$\sum_{n=1}^{509}\left[\frac{2n}{509}\right]=\sum_{n=1}^{254}\left[\frac{2n}{509}\right]+\sum_{n=255}^{508}\left[\frac{2n}{509}\right]+\left[\frac{2\times 509}{509}\right]$

$=0\times 254+1\times 254+2=256$.

而$\sum_{n=1}^{509}n=\frac{1}{2}\cdot 509\cdot 510=129795$.

故 $S=129795+256=130051$.

例 2 求$\left[\frac{1^2}{2006}\right]$，$\left[\frac{2^2}{2006}\right]$，…，$\left[\frac{2006^2}{2006}\right]$这 2006 个数中不同的值的个数.

分析 所给数显然都是区间$[0,2006]$内的整数，有些整数被取到不只一次，有些整数则一次都未取到，关键就是要找出这两类整数间的分界点.

解 对于任意 $n\in\{1,2,\cdots,2005\}$，当$\frac{(n+1)^2}{2006}-\frac{n^2}{2006}\geqslant 1$，

即 $n\geqslant 1004$ 时，$\left[\frac{(n+1)^2}{2006}\right]\geqslant\left[\frac{n^2}{2006}+1\right]=1+\left[\frac{n^2}{2006}\right]$，

故此时$\left[\frac{(n+1)^2}{2006}\right]$与$\left[\frac{n^2}{2006}\right]$取不同的值；

当$\frac{(n+1)^2}{2006}-\frac{n^2}{2006}<1$，即 $n\leqslant 1003$ 时，

$\left[\frac{(n+1)^2}{2006}\right]\leqslant\left[\frac{n^2}{2006}+1\right]=\left[\frac{n^2}{2006}\right]+1$，

而本来就有$\left[\frac{(n+1)^2}{2006}\right]\geqslant\left[\frac{n^2}{2006}\right]$，

故此时$\left[\frac{(n+1)^2}{2006}\right]=\left[\frac{n^2}{2006}\right]$或$\left[\frac{(n+1)^2}{2006}\right]=\left[\frac{n^2}{2006}\right]+1$.

上述结论意味着$\left[\frac{1004^2}{2006}\right]$，$\left[\frac{1005^2}{2006}\right]$，…，$\left[\frac{2006^2}{2006}\right]$这 1003 个数的值均不相同，即可取到 1003 个值.

$\left[\frac{1^2}{2006}\right]$，$\left[\frac{2^2}{2006}\right]$，…，$\left[\frac{1004^2}{2006}\right]$这 1004 个数可取到区间$\left[\left[\frac{1^2}{2006}\right],\left[\frac{1004^2}{2006}\right]\right]$内的任意一个整数.

即可取到 502 个值，这里$\left[\frac{1004^2}{2006}\right]$被算了两遍且$\left[\frac{1003^2}{2006}\right]\neq\left[\frac{1004^2}{2006}\right]$.

故所给 2006 个数共可取到 $1003+502-1=1504$ 个值.

例 3 求函数 $f(x)=[x]+[2x]+[3x]+\left[\frac{x}{2}\right]+\left[\frac{x}{3}\right]$在 $0\leqslant x\leqslant 100$ 上所取的不同的整数值的个数.

分析 易发现 $f(x+6)-f(x)$为定值，故不妨先考虑 $f(x)$在 $0\leqslant x<6$ 所取的不同的整数值的个数.

解 $f(x)$是阶梯函数，它的值要往上升，则至少要在点$[x]$，$[2x]$，$[3x]$，$\left[\frac{x}{2}\right]$，$\left[\frac{x}{3}\right]$之一处向上跳跃. 故向上升时，x 的值必是 1，或$\frac{1}{2}$，或$\frac{1}{3}$，或 2，或 3 的倍数，而在$[0,6)$内，共有 $0,\frac{1}{3},\frac{1}{2},\frac{2}{3},1,\frac{4}{3},\frac{3}{2},\frac{5}{3},2,\frac{7}{3},\frac{5}{2},\frac{8}{3},3,\frac{10}{3},\frac{7}{2},\frac{11}{3},4,\frac{13}{3},\frac{9}{2},\frac{14}{3},5,\frac{16}{3},\frac{11}{2},\frac{17}{3}$这 24 个数是 1，或$\frac{1}{2}$，或$\frac{1}{3}$，或 2，或 3 的倍数. 从而 $f(x)$在区间$[0,6)$上所取的不同值的个数是 24，在$[0,96)$上所取的不同值的个数是 $24\times16=384$. 又 $f(x)$在$[96,100]$上所取值的个数与在$[0,4]$上所取值的个数相同，在$[0,4]$上，$f(x)$有 17 次跳跃，故 $f(x)$在$[0,100]$上所取不同值的个数为 $384+17=401$.

例 4 求正整数$\left[\frac{10^{93}}{10^{31}+3}\right]$的末两位数字.

分析 将分数$\frac{10^{93}}{10^{31}+3}$写成带分数的形式使本题的解易得.

解 因为
$$\begin{aligned}10^{93}+3^3&=(10^{31})^3+3^3\\&=(10^{31}+3)(10^{62}-3\times10^{31}+9),\end{aligned}$$

从而原式 $=(10^{31})^2-3\times10^{31}+9+\left[\dfrac{-3^3}{10^{31}+3}\right]$

$$=10^{31}\times(10^{31}-3)+9-1$$

$$=10^{31}\times(10^{31}-3)+8.$$

故所求的末两位数字，十位是 0，个位是 8.

例 5 (2005 年全国高中数学联赛试题)定义函数

$$f(k)=\begin{cases}0, & k\text{ 为完全平方数}\\ \left[\dfrac{1}{\{\sqrt{k}\}}\right], & k\text{ 不为完全平方数}\end{cases}\text{，求}\sum_{k=1}^{240}f(k).$$

分析 k 不为完全平方数时，k 一定介于两个相邻的完全平方数之间，将$[1,240]$以完全平方数为分界点分成若干个区间，对属于每一个子区间的 k 分别对 $f(k)$进行求和.

解 $15^2<240<16^2$.

由于 k 为完全平方数时 $f(k)=0$，故

$$\sum_{k=1}^{240}f(k)=\sum_{k=1+1}^{2^2-1}f(k)+\sum_{k=2^2+1}^{3^2-1}f(k)+\cdots+\sum_{k=14^2+1}^{15^2-1}f(k)+\sum_{k=226}^{240}f(k)$$

$$=\sum_{n=1}^{14}\sum_{k=n^2+1}^{(n+1)^2-1}f(k)+\sum_{k=226}^{240}f(k).$$

当 $n^2+1\leqslant k\leqslant(n+1)^2-1$ 时，$[\sqrt{k}]=n$，$\{k\}=\sqrt{k}-[k]=\sqrt{k}-n$.

故 $\left[\dfrac{1}{\{\sqrt{k}\}}\right]=\left[\dfrac{1}{\sqrt{k}-n}\right]=\left[\dfrac{\sqrt{k}+n}{k-n^2}\right]=\left[\dfrac{[\sqrt{k}+n]}{k-n^2}\right]=\left[\dfrac{2n}{k-n^2}\right]$.

所以 $\displaystyle\sum_{k=n^2+1}^{(n+1)^2-1}f(k)=\sum_{k=n^2-1}^{(n+1)^2-1}\left[\dfrac{2n}{k-n^2}\right]=\sum_{i=1}^{2n}\left[\dfrac{2n}{i}\right]$,

$$\sum_{k=226}^{240}f(k)=\sum_{k=226}^{240}\left[\dfrac{2\cdot15}{k-15^2}\right]=\sum_{i=1}^{15}\left[\dfrac{30}{i}\right].$$

故 $\displaystyle\sum_{k=1}^{240}f(k)=\sum_{n=1}^{14}\sum_{i=1}^{2n}\left[\dfrac{2n}{i}\right]+\sum_{i=1}^{15}\left[\dfrac{30}{i}\right]$

$$=\sum_{n=1}^{14}\left(\sum_{i=1}^{n}\left[\dfrac{2n}{i}\right]+\sum_{i=n+1}^{2n}\left[\dfrac{2n}{i}\right]\right)+\sum_{i=1}^{15}\left[\dfrac{30}{i}\right]$$

$$=\sum_{n=1}^{14}\left(\sum_{i=1}^{n}\left[\dfrac{2n}{i}\right]+n\right)+\sum_{i=1}^{15}\left[\dfrac{30}{i}\right]$$

$$=\sum_{n=1}^{14}\sum_{i=1}^{n}\left[\dfrac{2n}{i}\right]+\sum_{i=1}^{15}\left[\dfrac{30}{i}\right]+\sum_{n=1}^{14}n$$

$$=\sum_{n=1}^{15}\sum_{i=1}^{n}\left[\dfrac{2n}{i}\right]+105.$$

设 $T_n=\displaystyle\sum_{i=1}^{n}\left[\dfrac{2n}{i}\right]$，$1\leqslant n\leqslant15$.

则 $T_1=\left[\frac{2}{1}\right]=2, T_2=\left[\frac{4}{1}\right]+\left[\frac{4}{2}\right]=4+2=6$，

$T_3=\left[\frac{6}{1}\right]+\left[\frac{6}{2}\right]+\left[\frac{6}{3}\right]=6+3+2=11$，

$T_4=\left[\frac{8}{1}\right]+\left[\frac{8}{2}\right]+\left[\frac{8}{3}\right]+\left[\frac{8}{4}\right]=8+4+2\times 2=16$，

$T_5=\left[\frac{10}{1}\right]+\left[\frac{10}{2}\right]+\cdots+\left[\frac{10}{5}\right]=10+5+3+2\times 2=22$，

$T_6=\left[\frac{12}{1}\right]+\left[\frac{12}{2}\right]+\cdots+\left[\frac{12}{6}\right]=12+6+4+3+2\times 2=29$，

$T_7=\left[\frac{14}{1}\right]+\left[\frac{14}{2}\right]+\cdots+\left[\frac{14}{7}\right]=14+7+4+3+2\times 3=34$，

$T_8=\left[\frac{16}{1}\right]+\left[\frac{16}{2}\right]+\cdots+\left[\frac{16}{8}\right]=16+8+5+4+3+2\times 3=42$，

$T_9=\left[\frac{18}{1}\right]+\left[\frac{18}{2}\right]+\cdots+\left[\frac{18}{9}\right]=18+9+6+4+3\times 2+2\times 3=49$，

$T_{10}=\left[\frac{20}{1}\right]+\left[\frac{20}{2}\right]+\cdots+\left[\frac{20}{10}\right]=20+10+6+5+4+3+2\times 4=56$，

$T_{11}=\left[\frac{22}{1}\right]+\left[\frac{22}{2}\right]+\cdots+\left[\frac{22}{11}\right]=22+11+7+5+4+3\times 2+2\times 4=63$，

$T_{12}=\left[\frac{24}{1}\right]+\left[\frac{24}{2}\right]+\cdots+\left[\frac{24}{12}\right]=24+12+8+6+4\times 2+3\times 2+2\times 4=72$，

$T_{13}=\left[\frac{26}{1}\right]+\left[\frac{26}{2}\right]+\cdots+\left[\frac{26}{13}\right]=26+13+8+6+5+4+3\times 2+2\times 5=78$，

$T_{14}=\left[\frac{28}{1}\right]+\left[\frac{28}{2}\right]+\cdots+\left[\frac{28}{14}\right]=28+14+9+7+5+4\times 2+3\times 2+2\times 5=87$，

$T_{15}=\left[\frac{30}{1}\right]+\left[\frac{30}{2}\right]+\cdots+\left[\frac{30}{15}\right]=30+15+10+7+6+5+4+3\times 3+2\times 5=96$，

$$\begin{aligned}故\sum_{k=1}^{240} f(k)&=\sum_{n=1}^{15} T_n+105\\&=2+6+11+16+22+29+34+42+49+56+63+72+78+87+96+105\\&=768.\end{aligned}$$

例 6　证明由 $a_n=[n\sqrt{2}]$ 定义的序列 $\{a_n\}$ 中，有无穷多个项是 2 的整数幂.

分析与解　我们需构造满足其性质的一类正整数 n 满足条件，同时满足这种性质的正整数有无穷多个.

构造集合 $A=\left\{a \mid \left\{\frac{2^a}{\sqrt{2}}\right\}>1-\frac{\sqrt{2}}{2}, a\in \mathbf{N}_+\right\}, B=\left\{b \mid b=\left[\frac{2^a}{\sqrt{2}}\right]+1, a\in A\right\}$.

则对任意 $b\in B$ 而言，存在 $a\in \mathbf{N}_+$ 使得 $b=\left[\frac{2^a}{\sqrt{2}}\right]+1$，

$$a_b=[b\sqrt{2}]=\left[\sqrt{2}\cdot\left(\left[\frac{2^a}{\sqrt{2}}\right]+1\right)\right]=\left[\sqrt{2}\cdot\left(\frac{2^a}{\sqrt{2}}-\left\{\frac{2^a}{\sqrt{2}}\right\}+1\right)\right]$$

$$=\left[2^a+\sqrt{2}-\sqrt{2}\cdot\left\{\frac{2^a}{\sqrt{2}}\right\}\right]=2^a+\left[\sqrt{2}-\sqrt{2}\cdot\left\{\frac{2^a}{\sqrt{2}}\right\}\right].$$

这里由 $a\in A$ 知 $\left\{\frac{2^a}{\sqrt{2}}\right\}>1-\frac{\sqrt{2}}{2}$，而 $\left\{\frac{2^a}{\sqrt{2}}\right\}<1$.

所以 $\sqrt{2}-\sqrt{2}\cdot 1<\sqrt{2}-\sqrt{2}\cdot\left\{\frac{2^a}{\sqrt{2}}\right\}<\sqrt{2}-\sqrt{2}\times\left(1-\frac{\sqrt{2}}{2}\right)$，

即 $0<\sqrt{2}-\sqrt{2}\cdot\left\{\frac{2^a}{\sqrt{2}}\right\}<1$，故 $\left[\sqrt{2}-\sqrt{2}\cdot\left\{\frac{2^a}{\sqrt{2}}\right\}\right]=0$.

所以 $a_b=2^a$，是 2 的整数幂.

下面我们只需证明 B 是无限集.

假设 A 为有限集，则存在 A 中的最大项 m_1，

即 $\left\{\frac{2^{m_1}}{\sqrt{2}}\right\}>1-\frac{\sqrt{2}}{2}$，且对任意 $m>m_1$，均有 $\left\{\frac{2^m}{\sqrt{2}}\right\}\leqslant 1-\frac{\sqrt{2}}{2}$.

于是 $\left\{\frac{2^{m_1+1}}{\sqrt{2}}\right\}\leqslant 1-\frac{\sqrt{2}}{2}<\frac{1}{2}$，

$$\left\{\frac{2^{m_1+2}}{\sqrt{2}}\right\}=\left\{2\times\frac{2^{m_1+1}}{\sqrt{2}}\right\}$$

$$=\left\{2\times\left(\left[\frac{2^{m_1+1}}{\sqrt{2}}\right]+\left\{\frac{2^{m_1+1}}{\sqrt{2}}\right\}\right)\right\}=\left\{2\times\left[\frac{2^{m_1+1}}{\sqrt{2}}\right]+2\times\left\{\frac{2^{m_1+1}}{\sqrt{2}}\right\}\right\}$$

$$=\left\{2\times\left\{\frac{2^{m_1+1}}{\sqrt{2}}\right\}\right\}=2\times\left\{\frac{2^{m_1+1}}{\sqrt{2}}\right\}.$$

同理可得 $\left\{\frac{2^{m_1+3}}{\sqrt{2}}\right\}=2\times\left\{\frac{2^{m_1+2}}{\sqrt{2}}\right\}$，$\left\{\frac{2^{m_1+4}}{\sqrt{2}}\right\}=2\times\left\{\frac{2^{m_1+3}}{\sqrt{2}}\right\}$，…，$\left\{\frac{2^{m_1+k+1}}{\sqrt{2}}\right\}=2\times\left\{\frac{2^{m_1+k}}{\sqrt{2}}\right\}$，$k\in\mathbf{N}_+$.

所以 $\left\{\frac{2^{m_1+k+1}}{\sqrt{2}}\right\}=2^k\times\left\{\frac{2^{m_1+1}}{\sqrt{2}}\right\}$，$k\in\mathbf{N}_+$.

但事实上由 $\left\{\frac{2^{m_1+1}}{\sqrt{2}}\right\}>0$ 知令 k 取到充分大的正整数后，$\left\{\frac{2^{m_1+k+1}}{\sqrt{2}}\right\}$ 的值也可取到充分大的数，与 $\left\{\frac{2^{m_1+k+1}}{\sqrt{2}}\right\}<1$ 相矛盾！

故假设不成立，即 A 为无限集.

而对任意 $a_1, a_2\in A, a_1<a_2$ 而言，有 $\frac{2^{a_2}}{\sqrt{2}}\geqslant 2\times\frac{2^{a_1}}{\sqrt{2}}>2$.

从而 $\frac{2^{a_2}}{\sqrt{2}}-\frac{2^{a_1}}{\sqrt{2}}\geqslant\frac{2^{a_1}}{\sqrt{2}}>1$, $\left[\frac{2^{a_2}}{\sqrt{2}}\right]\geqslant\left[\frac{2^{a_1}}{\sqrt{2}}\right]+1$.

所以 $\left[\frac{2^{a_2}}{\sqrt{2}}\right]+1\neq\left[\frac{2^{a_1}}{\sqrt{2}}\right]+1$.

这样一来，我们便建立了 A 到 B 的一一映射，故由 A 为无限集知 B 也为无限集. 即有无穷多个正整数 n 使得 $[\sqrt{2}n]$ 是 2 的整数幂.

评注 本题的解答用到了如下事实，对任意 $x\in\mathbf{R}$，若有 $\{x\}<\frac{1}{2}$，则有 $\{2x\}=2\{x\}$.

能力训练

一、选择题

1. 条件 $[x]=[y]$ 是条件 $|x-y|<1$ 的(　　)

A. 充分不必要条件　　B. 必要不充分条件

C. 充要条件　　D. 既不充分也不必要的条件

2. $[(\sqrt{3}+\sqrt{2})^{2006}]$ 的个位数字是(　　)

A. 0　　B. 1　　C. 8　　D. 9

3. 函数 $f(x)=[x]+[2x]+\left[\frac{5x}{3}\right]+[3x]+[4x]$, $x\in[0,100]$，则 $f(x)$ 的值域的元素个数为(　　)

A. 734　　B. 733　　C. 701　　D. 700

4. 每一个大于 2 的正整数 n 都可以表示成若干个两两不等的正整数的和，这个数的最大值为 $A(n)$，用 n 表示 $A(n)$ 为(　　)

A. $\left[\frac{\sqrt{8n+1}-1}{2}\right]$　B. $\left[\frac{\sqrt{8n+1}+1}{2}\right]$　C. $\left[\frac{\sqrt{8n+3}-1}{2}\right]$　D. $\left[\frac{\sqrt{8n+3}+1}{2}\right]$

5. 求 $\sum_{i=1}^{2006}\left(\frac{1}{[\sqrt[4]{(i+2)(i+3)}]}-\frac{1}{[\sqrt[4]{i(i+5)}]}\right)$ 的值，得到(　　)

A. -1　　B. 1　　C. 0　　D. $-\frac{1}{2}$

6. 定义数列 $\{a_n\}$: $a_1=1, a_2=2, a_{n+2}=a_n+a_{n+1}, n\in\mathbf{N}_+$，则 $\left[\frac{a_2}{a_1}\right]\cdot\left\{\frac{a_3}{a_2}\right\}\cdot\left\{\frac{a_4}{a_3}\right\}\cdot\cdots$

$\cdot\left\{\frac{a_{99}}{a_{98}}\right\}\cdot\left[\frac{a_{98}}{a_2}\right]$的值为(　　)

A. 2　　　B. 0　　　C. 1　　　D. $\frac{1}{2}$

二、填空题

7. 设 n 是给定的大于 1 的正整数，共有________个正整数 $A<n^2$，使得 $n\left|\left[\frac{n^2}{A}\right]+1\right.$.

8. $\sum\limits_{k=1}^{2006}\frac{1}{[\sqrt{k}]}-\sum\limits_{k=1}^{44}\frac{1}{k}$的值为________.

9. 和式 $S=\sum\limits_{n=1}^{502}\left[\frac{305n}{503}\right]$的值为________.

10. 前 1000 个正整数中可以表示成$[2x]+[4x]+[6x]+[8x]$的正整数有________个.

11. 设 $x>0$，则函数 $f(x)=\frac{x+x^{-1}}{[x]\cdot[x^{-1}]+[x]+[x^{-1}]+1}$的值域是________.

12. 设 a 是方程 $x^3-3x^2+1=0$ 的最大正根，则$[a^n]$($1\leqslant n\leqslant 2006$)这 2006 个数中共有________个可以被 17 整除.

三、解答题

13. 数列$\{a_n\}$定义如下：$a_n=[\sqrt{2}n]$，$n=0,1,2,\cdots$，证明：此数列中含有无穷多个完全平方数.

14. 若 n 历遍所有正整数，证明：$f(n)=\left[n+\sqrt{\frac{n}{3}}+\frac{1}{2}\right]$历遍所有正整数，但数列 $a_n=3n^2-2n$ 的项除外.

15. 对任意的 $n\in\mathbf{N}_+$，计算和 $S=\sum\limits_{k=0}^{\infty}\left[\frac{n+2^k}{2^{k+1}}\right]$.

§5.2　高斯方程与不等式

知识扫描

在求证含高斯函数的等式或不等式的时候，常用到以下的方法，第一步是将所讨论的数转移到(0,1)中来；第二步是把(0,1)分成若干段小区间来考虑，具体的分法因题而

异.

讨论含有高斯函数的方程是否有解，或确定它有多少解，解是什么，是高中数学竞赛中的常见题型. 处理此类问题时要综合高斯函数的性质及不等式等知识.

例题分析

例 1 设 $x\geqslant 0$，求证：$[\sqrt{[\sqrt{x}]}]=[\sqrt[4]{x}]$.

分析 利用$\sqrt[4]{x}\leqslant[\sqrt[4]{x}]<\sqrt[4]{x}+1$ 即可得到证明.

证明 设$[\sqrt[4]{x}]=a$，则由 $x\geqslant 0$ 和 a 为非负整数，

因此 $a^2\leqslant\sqrt{x}<(a+1)^2$.

又因为 a^2 与$(a+1)^2$ 均为整数，故 $a^2\leqslant[\sqrt{x}]<(a+1)^2$.

从而 $a\leqslant\sqrt{[\sqrt{x}]}<a+1$，故$[\sqrt{[\sqrt{x}]}]=a$，即$[\sqrt{[\sqrt{x}]}]=[\sqrt[4]{x}]$.

例 2 （2003 年克罗地亚国家数学竞赛题）对任意整数 $n(n>2)$，证明：$\left[\frac{n(n+1)}{4n-2}\right]=\left[\frac{n+1}{4}\right]$.

分析 当高斯函数内出现分数且分母为较小的正整数时，不少情况下要对未知数除以这个分母的余数进行讨论.

证明 由于
$$\frac{n(n+1)}{4n-2}=\frac{n(n+1)-\frac{n+1}{4}\times(4n-2)}{4n-2}+\frac{n+1}{4}$$
$$=\frac{\frac{1}{2}(n+1)}{4n-2}+\frac{n+1}{4}=\frac{n+1}{4(2n-1)}+\frac{n+1}{4},$$

而当 $n>2$ 时，$0<\frac{n+1}{4(2n-1)}<\frac{1}{4}$，

故$\frac{n(n+1)}{4n-2}<\frac{n+1}{4}+\frac{1}{4}$，且$\frac{n(n+1)}{4n-2}>\frac{n+1}{4}$.

故$\left[\frac{n+1}{4}\right]\leqslant\left[\frac{n(n+1)}{4n-2}\right]$. ①

下面证明

$\frac{n(n+1)}{4n-2}<\left[\frac{n+1}{4}\right]+1,(n>2)$ ②

分两种情况讨论

(1)令 $n=4k+r, r=0,1,2$,则有

$$\left[\frac{n+1}{4}\right]+1=k+1=\frac{n-r}{4}+1=\frac{n+(3-r)}{4}+\frac{1}{4}\geqslant\frac{n+1}{4}+\frac{1}{4},$$

结合$\frac{n(n+1)}{4n-2}<\frac{n+1}{4}+\frac{1}{4}$即知②成立.

(2)令 $n=4k+3$,则有

$$\left[\frac{n+1}{4}\right]+1=k+2>k+1+\frac{1}{4}=\frac{n+1}{4}+\frac{1}{4},$$

结合$\frac{n(n+1)}{4n-2}<\frac{n+1}{4}+\frac{1}{4}$即知②成立.

在两种情况下,不等式②均成立.

由②知$\left[\frac{n(n+1)}{4n-2}\right]<\left[\frac{n+1}{4}\right]+1=\left[\frac{n+1}{4}\right]+1$.

故$\left[\frac{n(n+1)}{4n-2}\right]\leqslant\left[\frac{n+1}{4}\right]$.

结合①即知$\left[\frac{n(n+1)}{4n-2}\right]=\left[\frac{n+1}{4}\right]$.

评注 要证明$[m]=[n]$,我们只需证$[m]\leqslant[n]$与$[m]\geqslant[n]$同时成立.

例3 证明不等式$[\sqrt{\alpha}]+[\sqrt{\alpha+\beta}]+[\sqrt{\beta}]\geqslant[\sqrt{2\alpha}]+[\sqrt{2\beta}]$对任意不小于1的实数$\alpha$和$\beta$成立.

分析 原不等式中有5个高斯符号,很复杂,不易将α与β的值直接进行分段,故应该先进行适当放缩,去掉几个高斯符号.

证明 设$a=\sqrt{\alpha}, b=\sqrt{\beta}$,则原不等式可写为

$$[a]+[\sqrt{a^2+b^2}]+[b]\geqslant[\sqrt{2}a]+[\sqrt{2}b], \quad ①$$

这里由$\alpha\geqslant1,\beta\geqslant1$知$a\geqslant1,b\geqslant1$.

利用均值不等式$\sqrt{\frac{a^2+b^2}{2}}\geqslant\frac{a+b}{2}$,得

$$[\sqrt{a^2+b^2}]\geqslant\left[\frac{a+b}{\sqrt{2}}\right]\geqslant\left[\frac{\sqrt{2}}{2}a\right]+\left[\frac{\sqrt{2}}{2}b\right].$$

由此可知要证明①式只需证明不等式

$$[x]+\left[\frac{\sqrt{2}}{2}x\right]\geqslant[\sqrt{2}x] \quad ②$$

对任意实数$x\geqslant1$成立即可.

分下面5种情况进行讨论:

(1)当 $x\geqslant 2+\sqrt{2}$时，$\left(1-\frac{\sqrt{2}}{2}\right)x\geqslant 1$，故$\left[\left(1-\frac{\sqrt{2}}{2}\right)x\right]\geqslant 1$.

$$\text{因此}[x]+\left[\frac{\sqrt{2}}{2}x\right]>x-1+\frac{\sqrt{2}}{2}x-1=\sqrt{2}x+\left(1-\frac{\sqrt{2}}{2}\right)x-2$$

$$\geqslant[\sqrt{2}x]+\left[\left(1-\frac{\sqrt{2}}{2}\right)x\right]-2\geqslant[\sqrt{2}x]-1.$$

即$[x]+\left[\frac{\sqrt{2}}{2}x\right]>[\sqrt{2}x]-1$.

上式两边均为整数，故$[x]+\left[\frac{\sqrt{2}}{2}x\right]\geqslant[\sqrt{2}x]$.

(2)当 $2\sqrt{2}\leqslant x\leqslant 2+\sqrt{2}$时，$2\leqslant\frac{\sqrt{2}}{2}x<\sqrt{2}+1$，$4\leqslant\sqrt{2}x<2+2\sqrt{2}<5$.

故$[x]+\left[\frac{\sqrt{2}}{2}x\right]\geqslant 2+2=4$，$[\sqrt{2}x]=4$.

(3)当$\frac{3}{2}\sqrt{2}\leqslant x<2\sqrt{2}$时，$\frac{3}{2}\leqslant\frac{\sqrt{2}}{2}x<2$，$3\leqslant\sqrt{2}x<4$.

故$[x]+\left[\frac{\sqrt{2}}{2}x\right]=2+1=3$，$[\sqrt{2}x]=3$.

(4)当$\sqrt{2}\leqslant x<\frac{3}{2}\sqrt{2}$时，$1\leqslant\frac{\sqrt{2}}{2}x<\frac{3}{2}$，$2\leqslant\sqrt{2}x<3$.

故$[x]+\left[\frac{\sqrt{2}}{2}x\right]\geqslant 1+1=2$，$[\sqrt{2}x]=2$.

(5)当 $1\leqslant x<\sqrt{2}$时，$\frac{\sqrt{2}}{2}\leqslant\frac{\sqrt{2}}{2}x<1$，$\sqrt{2}\leqslant\sqrt{2}x<2$.

故$[x]+\left[\frac{\sqrt{2}}{2}x\right]=1+0=1$，$[\sqrt{2}x]=1$.

综上所述，对任意实数 $x\geqslant 1$，②式均成立. 故不等式①成立，证毕.

例 4　$x\in\mathbf{R}^+$，$n\in\mathbf{N}_+$，证明：$[nx]\geqslant\frac{[x]}{1}+\frac{[2x]}{2}+\frac{[3x]}{3}+\cdots+\frac{[nx]}{n}$.

分析　此题若用前面述说的分段讨论证明是很繁杂的，既然题目与 $n\in\mathbf{N}_+$ 有关，提示我们应该灵活运用数学归纳法进行证明.

证明　令 $A_k=[x]+\frac{[2x]}{2}+\cdots+\frac{[kx]}{k}$，$k=1,2,\cdots$，

由于 $A_1=[x]$，故 $n=1$ 时命题成立.

设 $n\leqslant k-1$($k\geqslant 2$，$k\in\mathbf{N}_+$)时命题成立，即有

$A_1 \leqslant [x], A_2 \leqslant [2x], \cdots, A_{k-1} \leqslant [(k-1)x]$.

因为 $A_k - A_{k-1} = \frac{[kx]}{k}$，即 $kA_k - kA_{k-1} = [kx]$ 对一切 k 成立.

所以 $kA_k - kA_{k-1} = [kx], (k-1)A_{k-1} - (k-1)A_{k-2} = [(k-1)x], \cdots, 2A_2 - 2A_1 = [2x], A_1 = [x]$.

上述 k 个式子相加得

$kA_k - (A_1 + A_2 + \cdots + A_{k-1}) = [x] + [2x] + \cdots + [(k-1)x] + [kx]$,

故
$$\begin{aligned} kA_k &= [x]+[2x]+\cdots+[(k-1)x]+[kx]+A_{k-1}+A_{k-2}+\cdots+A_2+A_1 \\ &\leqslant [x]+[2x]+\cdots+[(k-1)x]+[kx]+[(k-1)x]+[(k-2)x] \\ &\quad +\cdots+[2x]+[x] \\ &= ([x]+[(k-1)x])+([2x]+[(k-2)x])+\cdots+([(k-1)x] \\ &\quad +[x])+[kx] \leqslant [kx]+[kx]+\cdots+[kx]+[kx]=k[kx]. \end{aligned}$$

故 $A_k \leqslant [kx]$，即 $n=k$ 时命题成立.

故原不等式对一切 $n \in \mathbf{N}_+$ 均成立.

例 5 (2003～2004 年瑞典数学竞赛)求所有的实数 x，满足方程 $[x^2-2x]+2[x]=[x]^2$，其中 $[a]$ 表示不超过 a 的最大整数.

分析 $[x^2-2x]$ 这个式子较复杂，考虑用换元法对它进行化简.

解 令 $x=y+1$，则原方程变为

$[(y+1)^2-2(y+1)]+2[y+1]=[y+1]^2$,

即 $[y^2-1]+2[y+1]=[y+1]^2$,

亦即 $[y^2]-1+2[y]+2=[y]^2+2[y]+1$.

亦即 $[y^2]=[y]^2$.

设 $n=[y]$，则 $[y^2]=n^2$，故 $n^2 \leqslant y^2 < n^2+1$.

所以 $|n| \leqslant y < \sqrt{n^2+1}$ 或 $-\sqrt{n^2+1} < y \leqslant -|n|$.

当 $n \in \mathbf{N}$ 时，$n \leqslant y < \sqrt{n^2+1}$，满足 $n=[y]$;

当 $n \notin \mathbf{N}$ 即 $n \leqslant -1$ 时，$-\sqrt{n^2+1} < y \leqslant n$，结合 $n=[y]$ 知此时只能是 $y=n$.

故 $y \in \mathbf{Z} \cup [n, \sqrt{n^2+1})$ $(n \in \mathbf{N})$.

因此 $x \in \mathbf{Z} \cup [n+1, \sqrt{n^2+1}+1)$ $(n \in \mathbf{N})$.

例 6 使得等式 $x[x[x[x]]]=2006$ 成立的正实数 x 有多少个?

分析 利用 $x \leqslant [x] < x+1$ 逐步消去外部的高斯符号.

解 先假定存在满足 $x[x[x[x]]]=2006$ 的正实数 x.

若 $0 < x \leqslant 6$，则 $x[x[x[x]]] \leqslant 6 \cdot [6 \cdot [6 \cdot [6]]] = 1296 < 2006$;

若 $x \geqslant 7$，则 $x[x[x[x]]] \geqslant 7 \cdot [7 \cdot [7 \cdot [7]]] = 2401 > 2006$.

由此可知 $6<x<7$，$[x]=6$.

故 $2006=x[x[6x]]$.

但由 $x<7$ 知 $6x<42$，故 $[6x]\leqslant 41$.

所以 $x[6x]<7\times 41=287$.

所以 $[x[6x]]\leqslant 286$.

故 $x[x[6x]]<7\times 286=2002<2006$，矛盾!

所以使得等式 $x[x[x[x]]]=2006$ 成立的正实数 x 为 0 个.

例 7 设 $[x]$ 表示不大于 x 的最大整数，a 是方程 $x^2-mx-1=0$ 的正根，这里 m 为给定的正整数，试证：存在无穷多个正整数 n，满足方程

$$[an+ma[an]]=mn+(m^2+1)[an].$$

分析 a 本身满足 $a^2-ma-1=0$，即 $a=m+\dfrac{1}{a}$，利用此式对高斯符号内部的式子化简，最后得到的无穷多个正整数 n 的值应与 a 有关.

证明 由于 a 是方程 $x^2-mx-1=0$ 的正根，

故有 $a^2-ma-1=0$，即 $a-m-\dfrac{1}{a}=0$.

从而 $a=m+\dfrac{1}{a}>m$.

则对于每一个大于 a 的正整数 n，有

$$[an+ma[an]]-mn-(m^2+1)[an]$$

$$=\left[\left(m+\frac{1}{a}\right)n+m\left(m+\frac{1}{a}\right)[an]\right]-mn-(m^2+1)[an]$$

$$=\left[mn+m^2[an]+\frac{n}{a}+\frac{m}{a}[an]\right]-mn-(m^2+1)[an]$$

$$=\left[\frac{n}{a}+\frac{m}{a}[an]\right]-[an]$$

$$=\left[\frac{n}{a}+\frac{m}{a}(an-\{an\})\right]-[an]$$

$$=\left[n\left(\frac{1}{a}+m\right)-\frac{m}{a}\{an\}\right]-[an]=\left[na-\frac{m}{a}\{an\}\right]-[an]$$

$$=\left[na-[na]-\frac{m}{a}\{an\}\right]$$

$$=\left[\{na\}-\frac{m}{a}\{an\}\right]=\left[\frac{a-m}{a}\cdot\{an\}\right].$$

由 $a>m>0$ 知 $0<\dfrac{a-m}{a}<1$.

又 $0\leqslant\{na\}<1$，故 $0\leqslant\frac{a-m}{a}\cdot\{na\}<1$.

从而 $\left[\frac{a-m}{a}\{na\}\right]=0$，所以当 n 为大于 a 的正整数时，

$[an+ma[an]]-mn-(m^2+1)[an]=0$，

即 $[an+ma[an]]=mn+(m^2+1)[an]$.

而大于 a 的正整数有无穷多个，故原命题得证.

例 8 （2003 年保加利亚国家数学奥林匹克题）求所有满足条件 $4[an]=n+[a[an]]$ 的实数 a，其中 n 是任意正整数.

分析 由于 n 为任意正整数，故应对 n 进行适当的赋值，得到所需要的式子.

解 若 $a\leqslant 0$，则 $[an]\leqslant 0$，$a[an]\geqslant 0$.

于是 $n+[a[an]]\geqslant n+0>0\geqslant 4[an]$，矛盾！

所以 $a>0$.

于是 $4(an-1)<4[an]=n+[a[an]]\leqslant n+a^2n$，

且 $4an\geqslant 4[an]=n+[a[an]]>n+a(an-1)-1$，

所以 $4a>1+a^2-\frac{a+1}{n}$.

且 $4a<1+a^2+\frac{4}{n}$，即 $1+a^2-\frac{a+1}{n}<4a<1+a^2+\frac{4}{n}$.

令 $n\to+\infty$，可得 $1+a^2=4a$，

所以 $a=2-\sqrt{3}$ 或 $a=2+\sqrt{3}$.

再令 $n=1$，则 $4[a]=1+[a[a]]$，而 $a=2-\sqrt{3}$ 不满足 $4[a]=1+[a[a]]$. 故 $a\neq 2-\sqrt{3}$.

当 $a=2+\sqrt{3}$ 时，对任意 $n\in\mathbf{N}_+$，设 $\left[\frac{n}{a}\right]=b$，$\left\{\frac{n}{a}\right\}=c$.

则由 $1+a^2=4a$，知 $a=4-\frac{1}{a}$，故

$$n+[a[an]]=\left[n+a\left[4n-\frac{n}{a}\right]\right]$$

$$=[n+a(4n-b-1)]$$

$$=[a(4n-1+c)]=\left[\left(4-\frac{1}{a}\right)(4n-1+c)\right]$$

$$=\left[4(4n-1)-4\left(\frac{n}{a}-c\right)+\frac{1-c}{a}\right]$$

$$=4(4n-1-b)=4\left[4n-\frac{n}{a}\right]=4[an].$$

这意味着 $a=2+\sqrt{3}$ 符合条件.

因此,$a=2+\sqrt{3}$ 是唯一的解.

例 9 求所有实数对 (a,b),使对所有正整数 n 满足 $a[bn]=b[an]$,其中 $[x]$ 表示不超过 x 的最大整数.

分析 当 $a\neq b$ 且 $ab\neq 0$ 时,我们易猜测 a、b 均为整数,但是否真的如此,有待进一步证明.

解 假设 $a[bn]=b[an]$ 对所有正整数 n 成立,且 $ab\neq 0$,$a\neq b$,我们证明 a 与 b 都是整数.

由于对任意实数 x 均有 $2[x]\leqslant 2x<2[x]+2$,

所以 $2[x]=[2x]$,或 $2[x]+1=[2x]$.

下面证明对任意正整数 m,有

$[2^m a]=2^m[a]$ 及 $[2^m b]=2^m[b]$.

$n=2$ 时,有 $a[2b]=b[2a]$.

如果 $[2a]=2[a]+1$,

则 $a[2b]=b[2a]=(2[a]+1)\cdot b=2[a]b+b=2a[b]+b$.

故 $[2b]=2[b]+\dfrac{b}{a}$.

又由 $2[b]=[2b]$,或 $2[b]+1=[2b]$ 知 $\dfrac{b}{a}=0$ 或 1.

但 $b\neq 0$,$a\neq b$,即 $\dfrac{b}{a}\neq 0,1$,矛盾!

因此 $[2a]\neq 2[a]+1$,即 $[2a]=2[a]$,同理可得 $[2b]=2[b]$.

故 $m=1$ 时,命题成立.

设对正整数 m,有 $[2^m a]=2^m[a]$,$[2^m b]=2^m[b]$.

当 $n=2^{m+1}$ 时,有 $a[2^{m+1}b]=b[2^{m+1}a]$.

如果 $[2^{m+1}a]=2[2^m a]+1$,

则 $a[2^{m+1}b]=b[2^{m+1}a]=2[2^m a]b+b$

$$=2^{m+1}[a]b+b=2^{m+1}a[b]+b.$$

故 $[2^{m+1}b]=2^{m+1}[b]+\dfrac{b}{a}$.

又由 $2[2^m b]=[2^{m+1}b]$,或 $2[2^m b]+1=[2^{m+1}b]$,及 $[2^m b]=2^m[b]$ 知

$[2^{m+1}b]=2[2^m b]=2^{m+1}[b]$,或 $[2^{m+1}b]=2[2^m b]+1=2^{m+1}[b]+1$.

所以 $\dfrac{b}{a}=0$ 或 1,即 $b=0$ 或 $a=b$,矛盾!

因此$[2^{m+1}a]=2^{m+1}[a]$，同理可证$[2^{m+1}b]=2^{m+1}[b]$.

于是，我们证明了对所有正整数 m 均有

$[2^m a]=2^m[a]$及$[2^m b]=2^m[b]$成立.

所以 $2^m[a]\leqslant 2^m a<2^m[a]+1$，即$[a]\leqslant a<[a]+\frac{1}{2^m}$对所有正整数 m 成立，

令 $m\to+\infty$，即知 $a=[a]$.

同理可得 $b=[b]$，故 a 与 b 都是整数.

而当 $a=0$，或 $b=0$，或 $a=b$ 时显然有 $a[bn]=b[an]$对一切正整数 n 成立.

故所有满足条件的实数对(a,b)所组成的集合为$\{(a,b)\mid a=0$，或 $b=0$，或 $a=b$，或 $a、b\in\mathbf{Z}\}$.

评注 证明了$[x]\leqslant x$与$[x]\geqslant x$后，x 自然为整数了.

例 10 （2006 年国家集训队考试试题）设 $f(n)$满足 $f(0)=0$，$f(n)=n-f(f(n-1))$，$n=1,2,3,\cdots$试确定所有实系数多项式 $g(x)$，使得

$f(n)=[g(n)]$，$n=0,1,2,\cdots$

其中$[g(n)]$表示不超过 $g(n)$的最大整数.

分析 $g(x)$既然为实系数多项式，就应该先讨论 $g(x)$中最高次项的次数，次数应该不会高，然后构造一个满足条件的 $g(x)$，最后证明这样的多项式是唯一存在的.

解 (1)证明 $g(x)=ax+b$，$a,b\in\mathbf{R}$，$a\neq0$.

设 $g(x)=a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0$，$a_k\neq0$，

由条件知$[g(n)]=n-[g(g(n-1))]$， ①

因此$\frac{[g(n)]}{n^{k^2}}=\frac{n}{n^{k^2}}-\frac{[g(g(n-1))]}{n^{k^2}}$. ②

若 $k\geqslant2$，则令 $n\to+\infty$，有 $0=0-a_k^{k+1}$，与 $a_k\neq0$ 矛盾.

因此 $k\leqslant1$，又由①知 $g(x)$不能恒为常数，故 $k=1$.

即 $g(x)=a_1x+a_0$，$a_1\neq0$.

(2)证明 $g(x)=\alpha x+b$，$b\in\mathbf{R}$，这里 $\alpha=\frac{\sqrt{5}-1}{2}$.

由(1)知 $g(x)=ax+b$，$a,b\in\mathbf{R}$，$a\neq0$.

在②中令 $n\to+\infty$，有 $a=1-a^2$，故 $a=\frac{1\pm\sqrt{5}}{2}$.

下面我们只需证明 $a>0$.

为此，我们用数学归纳法证明 $0\leqslant f(n)\leqslant n$.

1)$n=0$ 时，$f(0)=0$，命题显然成立.

2)假设命题对$\leqslant n-1$ 的自然数均成立，即

$0\leqslant f(n-1)\leqslant n-1,0\leqslant f(n-2)\leqslant n-2,\cdots,0\leqslant f(1)\leqslant 1,0\leqslant f(0)=0$,

则有 $0\leqslant f(f(n-1))\leqslant f(n-1)\leqslant n-1$.

因此 $1\leqslant f(n)\leqslant n$，于是 $0\leqslant f(n)\leqslant n$.

故对所有 $n\in\mathbf{N}$ 均有 $0\leqslant f(n)\leqslant n$.

由 $0\leqslant f(n)\leqslant n,n\in\mathbf{N}$ 知 $a>0$，因此 $a=\dfrac{-1+\sqrt{5}}{2}=\alpha$.

即 $g(x)=\alpha x+b$.

(3)证明 $g(x)=\alpha x+\alpha$.

由(2)知 $f(n)=[g(n)]=[\alpha n+b]=[\alpha(n+1)+b-\alpha]$

$=[(\alpha(n+1)]+[\{\alpha(n+1)\}+b-\alpha]$.

下面我们证明对所有的 $n\geqslant 0$，有 $[\{\alpha(n+1)\}+b-\alpha]=0$，即要证 $f(n)=[\alpha(n+1)]$.

为此，我们只需证明对所有的 $n\in\mathbf{N}_+$ 有

$[(n+1)\alpha]=n-[([n\alpha]+1)\alpha]$,

设 $n\alpha=[n\alpha]+\delta$，则

$[(n+1)\alpha]=[[n\alpha]+\delta+\alpha]=[n\alpha]+[\delta+\alpha]$.

注意到 $\alpha^2+\alpha=1$.

$[([n\alpha]+1+\alpha)]=[(n\alpha-\delta+1)\alpha]=[n\alpha^2-\delta\alpha+\alpha]$

$=[n-n\alpha-\delta\alpha+\alpha]=[n-[n\alpha]-\delta-\delta\alpha+\alpha]$

$=n-[n\alpha]+[-\delta-\delta\alpha+\alpha]$

$=n-[(n+1)\alpha]+[\delta+\alpha]+[-\delta-\delta\alpha+\alpha]$.

因此只需证明 $[\delta+\alpha]+[-\delta-\delta\alpha+\alpha]=0$.

1)当 $\delta+\alpha\geqslant 1$ 时，由 $\delta+\alpha<2$ 知 $[\delta+\alpha]=1$.

$-\delta-\delta\alpha+\alpha=-\delta(1+\alpha)+\alpha<(\alpha-1)(\alpha+1)+\alpha=\alpha^2+\alpha-1=0$,

且 $-\delta-\delta\alpha+\alpha=-\delta(1+\alpha)+\alpha>-(1+\alpha)+\alpha=-1$,

因此 $[-\delta-\delta\alpha+\alpha]=-1=-[\delta+\alpha]$.

即 $[-\delta-\delta\alpha+\alpha]+[\delta+\alpha]=0$.

2)当 $\delta+\alpha<1$ 时，$[\delta+\alpha]=0$.

$-\delta-\delta\alpha+\alpha=-\delta(1+\alpha)+\alpha>(\alpha-1)(\alpha+1)+\alpha=\alpha^2+\alpha-1=0,-\delta-\delta\alpha+\alpha\leqslant\alpha<1$.

因此 $[-\delta-\delta\alpha+\alpha]=0$.

此时亦有 $[-\delta-\delta\alpha+\alpha]+[\delta+\alpha]=0$,

故 $[(n+1)\alpha]=n-[([n\alpha]+1)\alpha]$ 对一切 $n\in\mathbf{N}_+$ 均成立.

所以 $f(n)=[\alpha(n+1)]$，即 $[\{\alpha(n+1)\}+b-\alpha]=0$.

在 $[\{\alpha(n+1)\}+b-\alpha]=0$ 中令 $n=0$，知 $0\leqslant b\leqslant 1$.

若 $b-a<0$，我们将证明存在 n，使得 $\{a(n+1)\}<\frac{1}{2}(a-b)$.

此时 $[\{a(n+1)\}+b-a]\leqslant -1$.

若 $b-a>0$，我们将证明存在 n，使得 $\{a(n+1)\}>1-\frac{1}{2}(b-a)$，

此时 $[\{a(n+1)\}+b-a]\geqslant 1$.

为此要证明引理(狄利克雷定理).

设 $a=\frac{1}{2}(\sqrt{5}-1)$，$\epsilon>0$，则存在正整数 n_1，n_2 使得

$\{n_1 a\}<\epsilon$，$\{n_2 a\}>1-\epsilon$.

证明如下，设 N 为一正整数且 $\frac{1}{N}<\epsilon$.

考虑 $0,\{\alpha\},\{2\alpha\},\cdots,\{N\alpha\}$ 共 $N+1$ 个数，一定存在 $0\leqslant k,l\leqslant N$，$k\neq l$ 使得 $0<\{k\alpha\}-\{l\alpha\}<\frac{1}{N}$，即 $0<(k-l)\alpha-[k\alpha]+[l\alpha]<\frac{1}{N}$.

若 $k>l$，则 $0<\{(k-l)\alpha\}<\frac{1}{N}<\epsilon$.

此时设 L 为整数，使 $L\{(k-l)\alpha\}<1<(L+1)\{(k-l)\alpha\}$，

由于 $L(k-l)\alpha=L[(k-l)\alpha]+L\{(k-l)\alpha\}$，

故 $\{L(k-l)\alpha\}=L\{(k-l)\alpha\}>1-\{(k-l)\alpha\}>1-\epsilon$.

若 $k<l$，则 $-\frac{1}{N}<(l-k)\alpha+[k\alpha]-[l\alpha]<0$.

即 $-\frac{1}{N}<\{(l-k)\alpha\}-1<0$.

即 $1-\epsilon<1-\frac{1}{N}<\{(l-k)\alpha\}<1$.

取整数 T，使 $T(1-\{(l-k)\alpha\})<1<(T+1)(1-\{(l-k)\alpha\})$.

$$
\begin{aligned}
\text{则 } T(l-k)\alpha &= T[(l-k)\alpha]+T\{(l-k)\alpha\}\\
&=T[(l-k)\alpha]+T+T(\{(l-k)\alpha\}-1)\\
&=T[(l-k)\alpha]+T-1+1-T(1-\{(l-k)\alpha\}).
\end{aligned}
$$

因此 $\{T(l-k)\alpha\}=1-T(1-\{(l-k)\alpha\})<l-\{(l-k)\alpha\}<\frac{1}{N}<\epsilon$.

引理得证.

所以 $b-a=0$，即 $b=a$.

综上得到 $g(x)=\frac{1}{2}(\sqrt{5}-1)(x+1)$ 是满足条件的唯一多项式.

能力训练

一、选择题

1. 方程$[x]+\left[\frac{1}{x}\right]=3$有(　　)个解.

A. 2　　B. 4　　C. 8　　D. 无穷多个

2. 设m为一正整数，方程$x^2-[x^2]=\{x\}^2$在$[1,m]$上有(　　)个解.

A. 0　　B. $m(m-1)+1$　　C. m^2　　D. 无穷多个

3. 若实数r使得$\left[r+\frac{19}{100}\right]+\left[r+\frac{20}{100}\right]+\cdots+\left[r+\frac{91}{100}\right]=546$，则$[100r]$的值为(　　)

A. 740　　B. 714　　C. 743　　D. 717

4. 方程$[3x+1]=2x-\frac{1}{2}$的所有根的和为(　　)

A. -1　　B. -2　　C. $-\frac{5}{4}$　　D. 0

5. 使方程$\left[\frac{10^n}{x}\right]=2006$具有整数解$x$的最小的自然数$n$所处的区间为(　　)

A. $[1,6]$　　B. $[7,12]$　　C. $[13,18]$　　D. $[19,24]$

6. 能使$\left[\frac{n^2}{5}\right]$为素数的所有自然数$n$的倒数之和为(　　)

A. $\frac{9}{20}$　　B. $\frac{11}{30}$　　C. $\frac{5}{12}$　　D. $\frac{37}{60}$

二、填空题

7. 方程$3x^3-[x]=3$的实数解为________.

8. 方程$x^2-2x-3=12\cdot\left[\frac{x-1}{2}\right]$的解为________.

9. 方程$x^2-8[x]+7=0$的所有解为________.

10. 设正实数$a>1$，自然数$n\geqslant 2$，且方程$[ax]=x$恰有n个不同的解，则a的取值范围为________.

11. 方程$[\tan x]=2\cos^2 x$的解集为________.

12. 使$[\log_2 1]+[\log_2 2]+[\log_2 3]+\cdots+[\log_2 n]=2006$成立的正整数$n$组成的集合为________.

三、解答题

13. 解方程 $4x^2-40[x]+51=0$.

14. 求所有正整数 n 使得 $\min\limits_{k\in\mathbf{N}_+}\left(k^2+\left[\frac{n}{k^2}\right]\right)=2006$.

15. 求满足下列式子的所有自然数 a 和 b：$\left[\frac{a^2}{b}\right]+\left[\frac{b^2}{a}\right]=\left[\frac{a^2+b^2}{ab}\right]+ab$.

§5.3 高斯函数的应用

知识扫描

1. 设 $a,b\in\mathbf{Z},b>0$，若 $a=bq+r,0\leqslant r<b$，则 $q=\left[\frac{a}{b}\right],r=b\left\{\frac{a}{b}\right\}$；设 $a,b\in\mathbf{N}$，则 $1,2,\cdots,a$ 中，b 的倍数有 $\left[\frac{a}{b}\right]$ 个.

2. 把 $n!$ 中素数 p 的最高次方幂记为 $p(n!)$，则 $p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^k}\right]$，$p^k\leqslant n<p^{k+1}$.

证明 因为 p 为质数，如果 p 能整除 $n!$，那么 p 能整除 $1,2,\cdots,n$ 中的某数，而 $1,2,\cdots,n$ 中 p 的倍数是下面 $\left[\frac{n}{p}\right]$ 个数，$p,2p,\cdots,\left[\frac{n}{p}\right]p$.

于是 $n!$ 中 p 的最高次幂就是 $p\cdot 2p\cdot\cdots\cdot\left[\frac{n}{p}\right]p=\left[\frac{n}{p}\right]!\ p^{\left[\frac{n}{p}\right]}$ 中 p 的最高次幂，

因此 $p(n!)=\left[\frac{n}{p}\right]+p\left(\left[\frac{n}{p}\right]!\right)$，

依次类推，有

$$p\left(\left[\frac{n}{p}\right]!\right)=\left[\frac{\left[\frac{n}{p}\right]}{p}\right]+p\left(\left[\frac{\left[\frac{n}{p}\right]}{p}\right]!\right)=\left[\frac{n}{p^2}\right]+p\left(\left[\frac{n}{p^2}\right]!\right),$$

所以 $p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+p\left(\left[\frac{n}{p^2}\right]!\right)$.

因为 $p^k\leqslant n<p^{k+1}$，最后得 $\left[\frac{n}{p^{k+1}}\right]=0$，

于是 $p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^k}\right]$，其中 $p^k\leqslant n<p^{k+1}$.

特别地，$p(p^r!)=p^{r-1}+p^{r-2}+\cdots+1=\frac{p^r-1}{p-1}$.

3. 把 m 个元素分成 n 类($m>n$)，则当 $n\nmid m$ 时，至少有一类中含有至少 $\left[\frac{m}{n}\right]+1$ 个元素.

4. $n\in\mathbf{N}_+$，$n\geqslant2$，则 $\sum\limits_{k=2}^{n}[\sqrt[k]{n}]=\sum\limits_{k=2}^{n}[\log_k n]$.

证明 构造平面区域 $D=\{(x,y)\mid y^x\leqslant n,x\geqslant2,y\geqslant2\}$，并考虑 D 中整点的个数.

如果一列一列地数，$x=2$ 时有 $[\sqrt{n}]$ 个，$x=3$ 时有 $[\sqrt[3]{n}]$ 个，…，$x=n$ 时有 $[\sqrt[n]{n}]$ 个，故共有 $\sum\limits_{k=2}^{n}[\sqrt[k]{n}]$ 个.

如果一行一行地数，$y=2$ 时，有 $[\log_2 n]$ 个，$y=3$ 时有 $[\log_3 n]$ 个，…，$y=n$ 时有 $[\log_n n]$ 个，故共有 $\sum\limits_{k=2}^{n}[\log_k n]$ 个.

综上所述，原等式得证.

5. 设正无理数 x 与 y 满足 $\frac{1}{x}+\frac{1}{y}=1$.

求证两数列 $[x],[2x],\cdots,[nx],\cdots$ 与 $[y],[2y],\cdots,[ny],\cdots$ 合在一起恰好不重复地构成自然数集.

证明 易知 $x>1,y>1$，则必有

$[(k+1)x]-[kx]>1,[(k+1)y]-[ky]>1$，

从而可知数列

$$[x],[2x],\cdots,[nx],\cdots \quad ①$$

$$[y],[2y],\cdots,[ny],\cdots \quad ②$$

都是严格递增的.

假定存在某个整数 p 在数列①和②中重复出现，那么必存在两个整数 a 与 b，使得

$p=[ax]=[by]$，即 $p<ax<p+1,p<by<p+1$.

因为 x 和 y 都是无理数，则上面两个不等式中不可能有等号出现，由此得

$$p=\frac{p}{x}+\frac{p}{y}<a+b<\frac{p+1}{x}+\frac{p+1}{y}=p+1.$$

这时就出现在相邻整数 p 和 $p+1$ 之间还有整数 $a+b$ 的情形，但这是不可能的.

因此可知数列①与②中没有相同的整数.

再假定存在某个整数 p 在数列①与②中都不出现，那么也会存在两个整数 a 与 b，使得 $ax<p<p+1<(a+1)x,by<p<p+1<(b+1)y$.

由此可得$\frac{a}{p}+\frac{b}{p}<\frac{1}{x}+\frac{1}{y}=1<\frac{a+1}{p+1}+\frac{b+1}{p+1}$.

即 $a+b<p<p+1<a+b+2$.

这时,在 $a+b$ 与 $a+b+2$ 之间出现了两个整数,但这是不可能的.

因此不可能在数列①,②中有某个整数不出现.

综上,命题得证.

例题分析

例 1 k 是自然数,且$\frac{1001\cdot1002\cdot\cdots\cdot2005\cdot2006}{11^k}$是整数,$k$ 的最大值是多少?

分析 将分子补成 2006!,再减去多余的次数即可.

解 $\frac{1001\cdot1002\cdot\cdots\cdot2005\cdot2006}{11^k}=\frac{2006!}{11^k\cdot1000!}$.

2006! 中含素因子 11 的最高幂次为

$$\left[\frac{2006}{11}\right]+\left[\frac{2006}{11^2}\right]+\left[\frac{2006}{11^3}\right]=182+16+1=199.$$

1000! 中含素因子 11 的最高幂次为

$$\left[\frac{1000}{11}\right]+\left[\frac{1000}{11^2}\right]=90+8=98.$$

所以 k 的最大值为 $199-98=101$.

例 2 求证当且仅当存在某个正整数 k 使得 $n=2^{k-1}$ 时,2^{n-1}能整除 $n!$.

分析 用高斯函数表示 n 中含有因子 2 的个数,再用高斯函数中一些熟知的不等式进行放缩.

证明 对于任意给定的正整数 n,总可以找到正整数 k 使得 $2^{k-1}\leqslant n<2^k$. ①

因此 $n!$ 中含有因子 2 的个数 m 为

$$m=\left[\frac{n}{2}\right]+\left[\frac{n}{2^2}\right]+\left[\frac{n}{2^3}\right]+\cdots+\left[\frac{n}{2^{k-1}}\right].$$

由函数$[x]$的性质$[x]+[y]\leqslant[x+y]$得

$$m\leqslant\left[n\left(\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^{k-1}}\right)\right]=\left[n\left(1-\frac{1}{2^{k-1}}\right)\right]=\left[n-\frac{n}{2^{k-1}}\right].$$

由于 $1\leqslant\frac{n}{2^{k-1}}<2$,知

$$m\leqslant\left[n-\frac{n}{2^{k-1}}\right]\leqslant n-1. \qquad ②$$

如果 $2^{k-1}|n!$，由②知 $m=n-1$.

再由①知 $\frac{n}{2^{k-1}}=1$，即 $n=2^{k-1}$.

反之，如果 $n=2^{k-1}$，由 m 的定义知

$m=2^{k-2}+2^{k-3}+\cdots+2+1=2^{k-1}-1=n-1$.

即 $n!$ 中有 $n-1$ 个因数 2，从而 $2^{n-1}|n!$.

例 3 定义函数 $f(n)(n\in\mathbf{N}_+)$ 如下：

设 $\frac{(2n)!}{n!\ (n+1002)!}=\frac{A(n)}{B(n)}$.

这里 $A(n)$，$B(n)$ 是互素的正整数：

若 $B(n)=1$，则 $f(n)=1$；

若 $B(n)\neq 1$，则 $f(n)=B(n)$ 的最大素因数，

求证 $f(n)$ 的不同值只有有限个，并求出它的最大值.

分析 容易看出数值 1002 并非关键，故要将问题一般化.

证明 先证明下面的引理：

引理 设 n，a 是正整数，且设分数 $\frac{(2n)!}{n!\ (n+a)!}$ 被写成既约形式，则分母不能被任意大于 $2a$ 的素数整除.

证明如下，设 $x=\frac{(2n)!\ (2a)!}{n!\ (n+a)!}$，

任一素数 p 在 x 中的最大的幂为

$$\sum_{r\geqslant 1}\left(\left\{\left[\frac{2n}{p^r}\right]+\left[\frac{2a}{p^r}\right]\right\}-\left\{\left[\frac{n}{p^r}\right]+\left[\frac{n+a}{p^r}\right]\right\}\right). \qquad ①$$

由于对任意非负数 y，z，不等式

$$[2y]+[2z]\geqslant[y]+[y+z] \qquad ②$$

成立.

事实上，设 $y=[y]+\alpha$，$z=[z]+\beta$，$0\leqslant\alpha$，$\beta<1$.

则不等式②$\Leftrightarrow 2[y]+[2\alpha]+2[z]+[2\beta]\geqslant[y]+[y]+[z]+[\alpha+\beta]$

$$\Leftrightarrow[z]+[2\alpha]+[2\beta]\geqslant[\alpha+\beta], \qquad ③$$

由 $0\leqslant\alpha$，$\beta<1$ 得 $0\leqslant\alpha+\beta<2$，于是 $[\alpha+\beta]=0$ 或 1.

若 $[\alpha+\beta]=0$，则③显然成立.

若 $[\alpha+\beta]=1$，则 α，β 中至少有一个不小于 $\frac{1}{2}$，从而 $[2\alpha]$ 与 $[2\beta]$ 中至少有一个为 1，③它成立.

从而证得②成立.

由②知①中每一项均不小于 0，故 x 为整数.

从而$\frac{x}{(2a)!}$的分母不可能包含任意大于 $2a$ 的素数，引理得证.

由引理及 $f(n)$的定义可得 $f(n)<2004$.

从而 $f(n)$的值只有有限个.

小于 2004 的最大素数为 2003.

当 $n=1001$ 时，$\frac{(2n)!}{n!\ (n+1002)!}=\frac{(2002)!}{1001!\ (2003)!}=\frac{1}{2003\cdot 1001!}$，

所以 $B(1001)=2003\cdot 1001!$.

因为 2003 为素数，所以 $f(1001)=2003$.

因此 $f(n)$的最大值为 2003.

例 4 证明对一切整数 $n>1$，方程

$\frac{x^n}{n!}+\frac{x^{n-1}}{(n-1)!}+\cdots+\frac{x^2}{2!}+\frac{x}{1!}+1=0$ 没有有理根.

证明 首先证明，对每个正整数 k 及每个素数 p，$p^k \nmid k!$.

设 $s\geqslant 0$ 为整数，满足 $p^s\leqslant k<p^{s+1}$，则满足 $p^r\,|\,k!$ 的最大整数 r 满足

$$r=\left[\frac{k}{p}\right]+\left[\frac{k}{p^2}\right]+\cdots+\left[\frac{k}{p^s}\right]\leqslant\frac{k}{p}+\frac{k}{p^2}+\cdots+\frac{k}{p^s}=k\cdot\frac{1-\frac{1}{p^s}}{1-\frac{1}{p}}\cdot\frac{1}{p}<k,$$

所以 $p^k \nmid k!$.

设方程$\frac{x^n}{n!}+\frac{x^{n-1}}{(n-1)!}+\cdots+\frac{x^2}{2!}+\frac{x}{1!}+1=0$， ①

有有理根 α，则

$$\alpha^n+n\alpha^{n-1}+\cdots+\frac{n!}{k!}\alpha^k+\cdots+\frac{n!}{2!}\alpha^2+\frac{n!}{1!}\alpha+n!\ =0,$$

设 $\alpha=\frac{c}{d}$，$c,d\in\mathbf{N}_+$，$(c,d)=1$，则

$$c^n+nc^{n-1}d+\cdots+\frac{n!}{1!}cd^{n-1}+n!\ d^n=0;\qquad ②$$

于是 $d\,|\,c$，从而 $d=1$.

即若方程①有有理根 α，则 α 必为整数.

设 p 为 n 的素因数，则由方程②知 $p\,|\,c^n$，即 $p\,|\,\alpha^n$，从而 $p\,|\,\alpha$.

设 r 为满足 $p^r\,|\,n!$ 的最大整数，则由 $p^k\,|\,\alpha^k$，$p^k\nmid k!$，

可得 $p^{r+1}\left|\frac{n!}{k!}\alpha^k\right.$，$k=1,2,\cdots,n$.

从而由②知 $p^{r+1}|n!$，矛盾！

故方程①没有有理根.

例 5 设 $p_1,p_2,p_3,\cdots$ 是依递增次序排列的素数，x_0 是 0 与 1 之间的实数，对正整数 k，定义

$$x_k=\begin{cases}0, & \text{若 } x_{k-1}=0\\ \left\{\dfrac{p_k}{x_{k-1}}\right\}. & \text{若 } x_{k-1}\neq 0\end{cases}$$

这里 $\{x\}$ 表示 x 的小数部分，求出一切 x_0 满足 $0<x_0<1$ 且使数列 $x_0,x_1,x_2,\cdots$ 中最终出现 0，并加以证明.

分析 当 x 为无理数时，$\dfrac{p}{x}$ 也为无理数（$p\in\mathbf{Q}$ 且 $p\neq 0$），从而 $\left\{\dfrac{p}{x}\right\}$ 也是无理数，故我们可以猜想 x_0 可取一切有理数.

解 我们证明，该数列最终出现 0，当且仅当 x_0 为有理数.

首先，我们证明对 $k\geqslant 1$，若 x_k 为有理数，则它的前一项 x_{k-1} 也是有理数.

若 $x_k=0$，则由题设知 $x_{k-1}=0$ 或 $\dfrac{p_k}{x_{k-1}}\in\mathbf{N}_+$，从而 x_{k-1} 为有理数.

若 $x_k\neq 0$，$x_k\in\mathbf{Q}$，则由

$$x_k=\left\{\frac{p_k}{x_{k-1}}\right\}=\frac{p_k}{x_{k-1}}-\left[\frac{p_k}{x_{k-1}}\right]，可得\ x_{k-1}=\frac{p_k}{x_k+\left[\dfrac{p_k}{x_{k-1}}\right]},$$

于是 x_{k-1} 也是有理数.

综上可知，对某个 k，若 x_k 为有理数，特别地，若数列最终出现 0，那么 x_0 也为有理数.

现在设 x_0 为有理数，那么数列 $x_0,x_1,x_2,\cdots$ 为有理数.

若 $x_{k-1}=\dfrac{m}{n}$，$0<m<n$，那么 $x_k=\left\{\dfrac{p_k}{\dfrac{m}{n}}\right\}=\left\{\dfrac{n\cdot p_k}{m}\right\}=\dfrac{r}{m}$，$0<r<m$.

这里 r 是 np_k 除以 m 的余数.

所以数列 $\{x_k\}$ 的每一个非零项的分母严格地小于前一项的分母，从而非零项的个数不超过 x_0 的分母.

因此，数列 $\{x_n\}$ 最终必出现 0.

例 6 设 $S(x)$ 表示数列 $\{[nx]\}$，$n\in\mathbf{N}_+$，证明方程 $x^3-10x^2+29x-25=0$，有相异的两实根 α,β，使 $S(\alpha)\cap S(\beta)$ 中有无穷多个正整数.

分析 方程有 3 个根，而题中只取了 α、β 两个根，故应将求的式子补全. 即计算 $|S(\alpha)\cap S(\beta)|+|S(\beta)\cap S(\gamma)|+|S(\gamma)\cap S(\alpha)|$ 的值，γ 为另外一个根.

证明 记 $f(x)=x^3-10x^2+29x-25$，则

$f(1)=-5<0, f(2)=1>0$,

$f(3)=-1<0, f(5)=-5<0, f(6)=5>0$.

于是方程 $f(x)=x^3-10x^2+29x-25=0$,在区间 $(1,2)$, $(2,3)$, $(5,6)$ 中各有一根,设这三个实根为 α,β,γ,则 $\alpha>0,\beta>0,\gamma>0$,且 $\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}=\frac{29}{25}$.

若用 $S'(\alpha)$, $S'(\beta)$, $S'(\gamma)$ 表示 $S(\alpha)$, $S(\beta)$, $S(\gamma)$ 中小于或等于 M(M 为任意给定的自然数)的数的集合,则

$$|S'(\alpha)|=\left[\frac{M}{\alpha}\right], |S'(\beta)|=\left[\frac{M}{\beta}\right], |S'(\gamma)|=\left[\frac{M}{\gamma}\right].$$

故 $|S'(\alpha)\cap S'(\beta)|+|S'(\beta)\cap S'(\gamma)|+|S'(\alpha)\cap S'(\gamma)|$ ①

$$\geqslant|S'(\alpha)|+|S'(\beta)|+|S'(\gamma)|-M$$

$$>M\left(\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}-1\right)-3$$

$$>\frac{4}{25}M-3.$$

由此可知,当 M 趋向于无穷时,①中的三项中必有一项趋向无穷,所以,必有满足方程的两实根(不妨设为 α 与 β),使得 $S(\alpha)\cap S(\beta)$ 中有无穷多个正整数.

例 7 设 $\alpha=\frac{r}{s}$,这里 r,s 是正整数,且 $r>s$, $(r,s)=1$,令集合 $N_\alpha=\{[n\alpha]\mid n=1,2,\cdots\}$,求证对任何 $m\in N_\alpha$, $r\nmid m+1$.

分析 $s=1$ 时 α 为正整数,应该单独讨论.

证明 分两种情况讨论:

(1)若 $s=1$,则 α 为正整数,$N_\alpha=\{rn\mid n=1,2,\cdots\}$,因为 $r>1$,则 $r\nmid rn+1$,而 $rn+1=m+1$,结论成立;

(2)若 $s>1$,由 $\frac{r}{s}>1$ 知

$$1\leqslant\left[\frac{r}{s}\right]<\left[\frac{2r}{s}\right]<\cdots<\left[\frac{(s-1)r}{s}\right]=\left[r-1+\frac{s-r}{s}\right]<r-1,\quad①$$

任取 $m=[n_0\alpha]\in N_\alpha$,令 $n_0=qs+k(0\leqslant k\leqslant s-1)$.

$$\text{则}[n_0\alpha]=\left[(qs+k)\cdot\frac{r}{s}\right]=[qr+k\alpha]=qr+[k\alpha],\quad②$$

由①知 $0\leqslant[k\alpha]<r-1$, $1\leqslant[k\alpha]+1<r$.

故由②知 $qr+1\leqslant m+1<(q+1)r=qr+r$.

所以 $r\nmid m+1$.

例 8 对实数 x,y,令 $s(x,y)=\{s\mid s=[nx+y], n\in\mathbf{N}\}$.

证明若 $r>1$ 为有理数，则存在实数 u,v，使得

$s(r,0)\cap s(u,v)=\varnothing$，$s(r,0)\cup s(u,v)=\mathbf{N}$.

证明 设 $r=\dfrac{p}{q}$，$p,q\in\mathbf{N}$，$p>q$，则

$u=\dfrac{p}{p-q}$及满足$-\dfrac{1}{p-q}\leqslant v<0$ 的 v 即为所求.

(1)如果 $s(r,0)\cap s(u,v)\neq\varnothing$，则存在一个 k 是 $s(r,0)$ 与 $s(u,v)$的公共元素，即 $k=[nr]=[mu+v]$.

因为 $r=\dfrac{p}{q}$，且 $k=\left[\dfrac{np}{q}\right]$，故$\dfrac{np}{q}=k+\left\{\dfrac{np}{q}\right\}$，$0\leqslant\left\{\dfrac{np}{q}\right\}<1$.

即 $np=kq+c$，$0\leqslant c\leqslant q-1$. ①

又由 $k=[mu+v]=\left[\dfrac{mp}{p-q}+v\right]$，知

$mp+v(p-q)=k(p-q)+d$，$0\leqslant d<p-q$， ②

由①＋②得$(m+n)p+v(p-q)=kp+c+d$， ③

因为$-\dfrac{1}{p-q}\leqslant v<0$，$p>q$，则 $v(p-q)<0$，

又 $c+d\geqslant 0$，于是由③得 $k<m+n$. ④

另一方面，由$-\dfrac{1}{p-q}\leqslant v$ 及①，②得 $v(p-q)\geqslant -1$，$c+d<p-1$.

则由③得$(m+n)p=kp-v(p-q)+(c+d)<kp+1+p-1=(k+1)p$.

从而 $m+n<k+1$， ⑤

④与⑤相矛盾. 所以 $s(r,0)\cap s(u,v)=\varnothing$.

(2)在 $n>m$ 时，$[nr]>[mr]$，$[nu+v]>[mu+v]$.

所以在 $s(u,v)$中没有相同的元素.

从而 $s(u,v)\cap\{1,2,\cdots,k-1\}$的元素个数等于满足$[mu+v]<k$ 的 m 的最大值 m_1，

即 m_1 满足$\begin{cases}m_1u+v<k,\\(m_1+1)u+v\geqslant k.\end{cases}$

解得$\dfrac{k-v}{u}-1\leqslant m_1<\dfrac{k-v}{u}$，即$\dfrac{u+v-k}{u}\geqslant -m_1>-\dfrac{k-v}{u}$.

所以 $m_1=-\left[\dfrac{u+v-k}{u}\right]$.

同样，$s(r,0)\cap\{1,2,\cdots,k-1\}$的元素个数 n_1，满足 $n_1=-\left[\dfrac{r-k}{r}\right]$.

于是有$-m_1-n_1\leqslant\dfrac{u+v-k}{u}+\dfrac{r-k}{r}=2-k+\dfrac{v(p-q)}{p}<2-k$.

所以 $m_1+n_1>k-2$，即 $m_1+n_1\geqslant k-1$.

又因为 $s(u,v)\cap s(r,0)=\varnothing$，故

$(s(u,v)\cup s(r,0))\cap\{1,2,\cdots,k-1\}=\{1,2,\cdots,k-1\}$.

此式对所有的 k 均成立.

因此 $s(u,v)\cup s(r,0)=\mathbf{N}$.

能力训练

1. 对于非负整数 x，函数 $f(x)$ 定义如下：

$$f(0)=0,\ f(x)=f\left(\left[\frac{x}{10}\right]\right)+\left[\lg\frac{10}{x-10\left[\frac{x-1}{10}\right]}\right].$$

$f(x)$ 在 $0\leqslant x\leqslant 2006$ 中取最大值时，x 的值是多少？

2. 试求出最大的正数 c，对于每个自然数 n，均有 $\{n\sqrt{2}\}\geqslant\frac{c}{n}$，确定使 $\{n\sqrt{2}\}=\frac{c}{n}$ 的自然数 n.

3. 设 a,b 为整数，n 为正整数，证明：$\dfrac{b^{n-1}a(a+b)(a+2b)\cdots[a+(n-1)b]}{n!}$ 为整数.

4. 设 m 为正整数，$m!$ 中所含因子 2 的个数记为 $n(m)$，求证存在自然数 $m>2006^{2006}$，使 $m=3^{2006}+n(m)$.

5. 数列 $\{a_n\}$ 按下列递推关系给出：$a_1=1,\ a_{n+1}=a_n+\dfrac{1}{[a_n]},\ n\geqslant 1$.

求使不等式 $a_n>20$ 成立的所有 n.

6. 设 n 是一个固定的正整数，$b(n)$ 是 $k+\dfrac{n}{k}$ 关于所有正整数 k 的最小值. 证明 $[b(n)]=[\sqrt{4n+1}]$.

7. 设 r,s,n 都是正整数，并且 $r+s=n$，试证：$A=\left\{\left[\dfrac{n}{r}\right],\left[\dfrac{2n}{r}\right],\cdots,\left[\dfrac{(r-1)n}{r}\right]\right\}$ 和 $B=\left\{\left[\dfrac{n}{s}\right],\left[\dfrac{2n}{s}\right],\cdots,\left[\dfrac{(s-1)n}{s}\right]\right\}$ 构成 $M=\{1,2,\cdots,n-2\}$ 的划分的充分必要条件是 r 和 s 都与 n 互素.

8. 设 m、n 是互质的正整数，且 m 为偶数，n 为奇数. 证明：和 $\dfrac{1}{2n}+\sum\limits_{k=1}^{n-1}(-1)^{\left[\frac{mk}{n}\right]}\left\{\dfrac{mk}{n}\right\}$ 不依赖于 m、n，其中 $[x]$ 为不超过 x 的最大整数，$\{x\}=x-[x]$.

第六章　无穷递降法

§6.1　用无穷递降法解不定方程

知识扫描

无穷递降法是证明某些不定方程无解时常用的方法，其证明模式大致为：首先假定原方程有解，然后构造某个无穷递降的过程，并且从方程本身看，这个过程应是有限的，从而导出矛盾. 无穷递降法的理论依据即是“最小数原理”，以下通过几个实例来说明无穷递降法在解不定方程中的应用.

例题分析

例 1　证明方程 $x^2+y^2+z^2+u^2=2xyzu$ 没有正整数解.

证明　假设原方程存在一组正整数解，设这组解为 $x=x_0, y=y_0, z=z_0, u=u_0$，则

$$x_0^2+y_0^2+z_0^2+u_0^2=2x_0y_0z_0u_0. \quad ①$$

由于 x_0, y_0, z_0, u_0 均为正整数，则由①的右边可以推知 x_0, y_0, z_0, u_0 中的奇数有偶数个，即或者 4 个，或者 2 个，或者 0 个. 如果所有这四个数都是奇数，则 $x_0^2+y_0^2+z_0^2+u_0^2$ 能被 4 整除(这是因为奇数的平方除以 4 余 1)，而 $2x_0y_0z_0u_0$ 不被 4 整除，矛盾；如果 x_0, y_0, z_0, u_0 中恰有两个奇数，则 $x_0^2+y_0^2+z_0^2+u_0^2$ 不被 4 整除，而 $2x_0y_0z_0u_0$ 能被 4 整除，矛

盾.所以全部4个数都为偶数,令 $x_0=2x_1, y_0=2y_1, z_0=2z_1, u_0=2u_1$,则 x_1, y_1, z_1, u_1 均为正整数,且由①知

$$(2x_1)^2+(2y_1)^2+(2z_1)^2+(2u_1)^2=2(2x_1)(2y_1)(2z_1)(2u_1),$$

即 $x_1^2+y_1^2+z_1^2+u_1^2=8x_1y_1z_1u_1$, ②

首先易知 x_1, y_1, z_1, u_1 中有偶数个奇数,而 x_1, y_1, z_1, u_1 不可能全是奇数,因为此时 $x_1^2+y_1^2+z_1^2+u_1^2$ 不能被8整除(奇数的平方除以8余1),同时也不能恰有2个奇数,因为此时 $x_1^2+y_1^2+z_1^2+u_1^2$ 也不能被8整除,于是,我们又得到 x_1, y_1, z_1, u_1 都是偶数,即 $x_1=2x_2, y_1=2y_2, z_1=2z_2, u_1=2u_2$ ($x_2, y_2, z_2, u_2\in\mathbf{N}_+$),则由②可得

$$x_2^2+y_2^2+z_2^2+u_2^2=32x_2y_2z_2u_2.$$

用与前面类似的方法,我们可以得出 x_2, y_2, z_2, u_2 是偶数,等等.如此继续推理下去,我们可以得知,对任意 $s\in\mathbf{N}_+$,有 $x_s^2+y_s^2+z_s^2+u_s^2=2^{2s+1}x_sy_sz_su_s$.

同时 $x_{s+1}=\frac{x_s}{2}, y_{s+1}=\frac{y_s}{2}, z_{s+1}=\frac{z_s}{2}, u_{s+1}=\frac{u_s}{2}$ 均为正整数,即 x_0 可以按上述方式(每次除以2)无穷递降下去,且递降后所得的数始终为正整数,这显然是不可能的(正整数集有最小元素1).

因此,方程 $x^2+y^2+z^2+u^2=2xyzu$ 无正整数解.

例2 证明不存在不同时为零,且满足方程 $x^2+y^2=3z^2$ 的整数 x, y, z.

证明 假设方程有整数解 $(x_0, y_0, z_0)\neq(0,0,0)$,

则 $x_0^2+y_0^2=3z_0^2$. ①

若 x_0, y_0 不能同时被3整除,则

$x_0^2+y_0^2\equiv1$ 或 $2 \pmod 3$. ②

这是因为对任一个不能被3整除的整数,它的平方除以3的余数都为1,而 x_0, y_0 中可能有1个或2个不能被3整除,于是有②式,而②与①矛盾.

所以 x_0, y_0 必同时能被3整除.

设 $x_0=3x_1, y_0=3y_1$ ($x_1, y_1\in\mathbf{Z}$),

代入①式可得:$(3x_1)^2+(3y_1)^2=3z_0^2$,所以 $z_0^2=3(x_1^2+y_1^2)$.

所以 $3\mid z_0$,可是 $z_0=3z_1$,代入上式($z_1\in\mathbf{Z}$).得 $x_1^2+y_1^2=3z_1^2$,

由以上推导可知,若 (x_0, y_0, z_0) 是原方程的一组不全为零的整数解,则 $\left(\frac{x_0}{3}, \frac{y_0}{3}, \frac{z_0}{3}\right)$ 也是原方程的一组不全为零的整数解,进一步可知 $\left(\frac{x_0}{3^2}, \frac{y_0}{3^2}, \frac{z_0}{3^2}\right)$ 也是原方程的一组不全为零的整数解……这样的变换可以无穷地进行下去,而由非零整数的性质知这是不可能的.

所以,方程 $x^2+y^2=3z^2$ 不存在不同时为零的整数解.

评注 通过以上两例我们可以看出"整除"通常是我们用来构造无穷递降过程的工

具.

例 3 设 a 是给定的正整数，A 和 B 是两个实数，试确定方程组

$$\begin{cases} x^2+y^2+z^2=(13a)^2 & ① \\ x^2(Ax^2+By^2)+y^2(Ay^2+Bz^2)+z^2(Az^2+Bx^2)=\frac{1}{4}(2A+B)(13a)^4 & ② \end{cases}$$

有正整数解的充分必要条件(用 A,B 的关系式表示，并予以证明).

解 原方程组有正整数解的充要条件是 $B=2A$，下面证明这个结论.

首先证明充分性，即已知 $B=2A$，证明原方程组有正整数解.

此时，我们可取 $x=12a,y=3a,z=4a$，这便是原方程组的一组正整数解.

再来证明必要性：将①代入②可得：

$$x^2(Ax^2+By^2)+y^2(Ay^2+Bz^2)+z^2(Az^2+Bx^2)=\frac{1}{4}(2A+B)(x^2+y^2+z^2)^2,$$

进而可得 $(2A-B)(x^4+y^4+z^4-2x^2y^2-2y^2z^2-2z^2x^2)=0$,

若 $2A\neq B$，则有 $x^4+y^4+z^4-2x^2y^2-2y^2z^2-2z^2x^2=0$,

即 $(x+y+z)(x+y-z)(x+z-y)(y+z-x)=0$,

不妨设 $x+y-z=0$，代入①式有

$$x^2+y^2+(x+y)^2=(13a)^2 \qquad ③$$

若有一组 $x_0,y_0,a_0(x_0,y_0,a_0\in\mathbf{N}_+)$ 使③成立，显然 a_0 为偶数，设 $a_0=2a'_0(a_0\in\mathbf{N}_+)$，此时 $4\mid x_0^2+y_0^2+(x_0+y_0)^2$，进而知 x_0,y_0 均为偶数(否则 $x_0^2+y_0^2+(x_0+y_0)^2\equiv 2(\bmod 4)$)，设 $x_0=2x'_0,y_0=2y'_0(x_0,y_0\in\mathbf{N}_+)$，于是有 $x'^2_0+y'^2_0+(x'_0+y'_0)^2=(13a'_0)^2$，这就得到 $\frac{x_0}{2},\frac{y_0}{2},\frac{a_0}{2}$ 也是③式的一组正整数组，将这一过程不断地进行下去，即可知对任意 $k\in\mathbf{N}_+$，都有 $2^k\mid a_0$，而 $a_0\in\mathbf{N}_+$，这显然是不可能的.

故若原方程组有正整数解，则必有 $2A=B$.

综上即知原方程组有正整数解的充分必要条件是 $B=2A$.

例 4 求不定方程 $x^4+y^4=z^2(xy\neq 0)$ 的正整数解. ①

证明 显见，只需证明①无正整数解.

用反证法来证明，假设方程①有正整数解，那么在全体正整数解中，必有一组解 x_0,y_0,z_0，使得 z_0 取得最小值. 下面我们由此找出一组正整数解 x_1,y_1,z_1 满足 $z_1<z_0$，从而得出矛盾.

(1) 首先必有 $(x_0,y_0)=1$，若不然，就有素数 p 使得 $p\mid x_0,p\mid y_0$，由此可以推知 $p^2\mid z_0^2$，所以 $p\mid z_0$，因此 $\frac{x_0}{p},\frac{y_0}{p},\frac{z_0}{p}$ 也是方程①的正整数解，但 $\frac{z_0}{p}<z_0$，这就和 z_0 的最小性矛盾. 因此必有 $(x_0,y_0)=1$，进而知 $(x_0,z_0)=1,(y_0,z_0)=1$，即 x_0,y_0,z_0 两两互质，又易知

x_0,y_0 必为一奇一偶(否则 $x_0^4+y_0^4\equiv 2\pmod 4$,注意 x_0,y_0 不可能同为偶数,即 $z_0^2\equiv 2\pmod 4$,矛盾).不妨设 $2\mid y_0$,则 z_0 为奇数.

(2)设 $g_0=(z_0-y_0^2,z_0+y_0^2)$,则 $g_0\mid(z_0-y_0^2+z_0+y_0^2,z_0+y_0^2-(z_0-y_0^2))$,

即 $g_0\mid(2z_0,2y_0^2)$,所以 $g_0\mid 2$.

又 y_0 与 z_0 异奇偶,所以 $z_0-y_0^2,z_0+y_0^2$ 均为奇数.

所以 $2\nmid g_0$,故 $g_0=1$.

由于 $x_0^4+y_0^4=z_0^2$,所以 $(z_0-y_0^2)(z_0+y_0^2)=x_0^4$.

由上式及 $(z_0-y_0^2,z_0+y_0^2)=1$,可以设

$z_0-y_0^2=u^4,z_0+y_0^2=v^4(u,v\in\mathbf{N}_+)$.

这里 $v>u>0,(u,v)=1,2\nmid uv$,进而有

$y_0^2=\dfrac{v^4-u^4}{2}=(v^2-u^2)\cdot\dfrac{(u^2+v^2)}{2}$.

(3)设 $g_2=\left(v^2-u^2,\dfrac{u^2+v^2}{2}\right)$(由 $2\nmid uv$ 知 u^2+v^2 为偶数).

则 $g_2\mid(v^2-u^2,u^2+v^2)$,

所以 $g_2\mid(v^2-u^2+u^2+v^2,u^2+v^2-(v^2-u^2))$.

即 $g_2\mid(2v^2,2u^2)$.

而 $(2v^2,2u^2)=2(v^2,u^2)=2$,所以 $g_2\mid 2$.

而由 $2\nmid uv$ 知 u,v 均为奇数,于是 $u^2+v^2\equiv 2\pmod 4$,则 $\dfrac{u^2+v^2}{2}$ 为奇数,所以 $2\nmid g_2$.所以 $g_2=1$.

又由 $y_0^2=(v^2-u^2)\cdot\dfrac{u^2+v^2}{2}$ 可以设

$v^2-u^2=a^2,\dfrac{u^2+v^2}{2}=b^2(a,b\in\mathbf{N}_+)$, ②

这里 $a>0,b>0,(a,b)=1$ 及 $2\mid a,2\nmid b$.

(4)由 u,v 满足条件及②式可推得 $0<b<v<z_0$,及 u,a,v 满足 $u^2+a^2=v^2$ 且 $2\mid a$,$(u,v)=1$.

因此可以得知存在 $r,s\in\mathbf{N}_+$,使得 $u=r^2-s^2,a=2rs,v=r^2+s^2$,

其中 $r>s>0,(s,r)=1,2\nmid r+s$.

由此及②式的第二个式子可得 $r^4+s^4=b^2$.

这表明 r,s,b 是方程①的正整数解,且 $b<z_0$.这和 z_0 的最小性矛盾,所以方程①无正整数解,进而知方程①没有 $xyz\neq 0$ 的正整数解.

评注 在本题的证明过程中由解 (x_0,y_0,z_0) 得到解 (r,s,b) 实质上就是对 z_0 进行了

一次递降,在这里我们通过赋予 b"最小性"从而导出矛盾,这种方法的思想精髓正是"无穷递降法".

例 5 正整数 a 与 b 使得 $\frac{a^2+b^2}{ab+1}=k(k\in\mathbf{N}_+)$,求证:$k$ 是某个正整数的平方.

分析 我们可以将 $\frac{a^2+b^2}{ab+1}=k$ 变形为 $a^2-kba+b^2-k=0$,则 a 是以 x 为元的一元二次方程 $x^2-kbx+b^2-k=0$ 的一个正整数根,由韦达定理可知该方程另一根为 $a'=kb-a=\frac{b^2-k}{a}$,则 $a'=kb-a$ 为整数且 a' 必不小于 0,否则由 $a'b<0$,知 $k=\frac{a'^2+b^2}{a'b+1}<0<\frac{a^2+b^2}{ab+1}=k$,矛盾! 于是我们又找到非负整数 a',b 使 $\frac{a'^2+b^2}{a'b+1}=k$,如果能在 a,b 与 a',b 之间建立某种递降关系,则本题就基本得到了解决.

证明 假设 k 不是完全平方数,则由条件可以得到不定方程

$$a^2-kab+b^2-k=0. \quad ①$$

显然,这个不定方程的解 (a,b) 不会使 $ab<0$,否则 $a^2+b^2=k(ab+1)\leqslant 0$,则有 $a=b=0$,与 $ab<0$ 不符.

设 (a,b) 是①的解中满足 $a,b\in\mathbf{N}_+$,且使 $a+b$ 最小的那个解,不妨设 $a\geqslant b$,固定 k 与 b,把①式视为以 a 为元的一元二次方程,它有一根为 a,设另一根为 a',由韦达定理有

$$\begin{cases} a+a'=kb & ② \\ aa'=b^2-k & ③ \end{cases}$$

由②式可知 a' 为整数,由③知 $a'\neq 0$(k 不为完全平方数).

又 ab 与 $a'b$ 均非负且 a,b 均为正整数,$a'\neq 0$,所以 $a'>0$.

所以 a' 为正整数,这时有

$$a'=\frac{b^2-k}{a}\leqslant\frac{b^2-1}{a}\leqslant\frac{a^2-1}{a}<a.$$

这时 (a',b) 为①的正整数解,$a',b\in\mathbf{N}_+$,但 $a'+b<a+b$,这与 (a,b) 的选法不合,得出矛盾,所以 k 必为一个正整数的平方.

能力训练

1. 证明四元二次不定方程 $x^2+y^2=3(u^2+v^2)$ 没有非零整数解.
2. 求方程 $x^2+y^2+z^2=x^2y^2$ 的整数解.
3. 求证:除 $a=b=c=d=0$ 外,方程 $6(6a^2+3b^2+c^2)=5d^2$ 没有别的整数解.

4. 设正整数 a,b,k 满足 $\frac{a^2+b^2}{ab-1}=k$，求证：$k=5$.

5. 证明两个平方数的和与差 $\begin{cases}y^2+z^2=t^2\\z^2-y^2=x^2\end{cases}$ 无正整数解.

6. 证明：不定方程 $x^4+y^2=z^4$ 没有正整数解.

7. 证明方程：$x^2+y^2-19xy-19=0$ 无整数解.

§6.2 无穷递降法的其他应用

知识扫描

在上一节中我们介绍了无穷递降法在解不定方程中的应用，在本节中，我们着重说明无穷递降法在数论、几何、组合中的应用.

例题分析

例 1 设 a,b,m 是正整数，$(a,b)=1$. 证明：在等差数列 $a+kb(k=0,1,2,3\cdots)$ 中，必有无穷多个数和 m 既约.

证明 由于 $(a+(k+m)b,m)=(a+kb,m)(k\in\mathbf{N}_+)$.

所以要证明在等差数列 $a+kb(k=0,1,2,\cdots)$ 中有无穷多个数和 m 既约，只需证明当 $k=0,1,2,\cdots,m-1$ 时，存在某个 k 使 $a+kb$ 与 m 互质.

设 c 是 m 的所有因数中满足 $(c,a)=1$ 的一个，并设 $d=(a+bc,m)$，如果 $d>1$.

由于 $(a,b)=1,(a,c)=1$，所以 $(a,bc)=1$.

又 $d\mid(a+bc)$，所以 $(d,a)=(d,bc)=1$.

由此及 $d\mid m,c\mid m$ 可以得知 $dc\mid m$.

于是，我们在 m 的所有因数中找到一个比 c 更大 $(dc>c)$ 且与 a 互质的数，如果当 $k\in\{0,1,2\cdots,m-1\}$ 时，恒有 $(a+bk,m)>1$，则以上过程可以无限地进行下去，即可以不断地找出 m 的新的因数，且该因数与 m 的差不断地缩小，而这显然是不可能的.

所以必存在某个 $k\in\{0,1,2,\cdots,m-1\}$ 使 $(a+kb,m)=1$，即 $a,a+b,a+2b,\cdots,a+(n-1)b$ 中至少有一个与 m 互质，进而可以得知所要证的结论成立.

例 2 正五边形的每个顶点对应一个整数使得这五个整数的和为正. 若其中三个相连顶点相应的整数依次为 x,y,z，而中间的 $y<0$，则要进行如下的操作：整数 x,y,z 分别换为 $x+y,-y,z+y$. 只要所得的五个整数中至少还有一个为负时，这种操作就继续进行. 问：是否这样的操作进行有限次后必定终止.

分析与解 题中所述的操作并不改变五边形顶点上各数之和，且这些数始终都为整数. 如果我们能构造出一个函数，该函数有下界且每进行一次操作，该函数的函数值都至少减小某个正值 $M(M>0)$，则问题便得到了解决，因此本题的关键就在于构造出一个符合要求的函数，由于要求所构造的函数有下界，则可联想到整数平方的非负性（也可考虑整数绝对值的非负性），于是可换如下方法构造函数 f：

设正五边形五个顶点上的数按顺时针顺次为 x_1,x_2,x_3,x_4,x_5，令 $f(x_1,x_2,x_3,x_4,x_5)=(x_1-x_3)^2+(x_2-x_4)^2+(x_3-x_5)^2+(x_4-x_1)^2+(x_5-x_2)^2$（注意，由于操作不改变五边形顶点上五数之和且最初所给的五个整数和为正，故有 $x_1+x_2+x_3+x_4+x_5\geqslant 1$）.

不妨对 x_5,x_1,x_2 进行了一次操作（$x_1<0$），此时五边形顶点上的数变为 $(-x_1,x_1+x_2,x_3,x_4,x_5+x_1)$.

此时，有

$$\begin{aligned}&f(-x_1,x_1+x_2,x_3,x_4,x_5+x_1)-f(x_1,x_2,x_3,x_4,x_5)\\&=(-x_1-x_3)^2+(x_1+x_2-x_4)^2+(x_3-(x_5+x_1))^2+(x_4-(-x_1))^2+(x_5+x_1-\\&\quad(x_1+x_2))^2-(x_1-x_3)^2-(x_2-x_4)^2-(x_3-x_5)^2-(x_4-x_1)^2-(x_5-x_2)^2\\&=2x_1(x_1+x_2+x_3+x_4+x_5)\\&\leqslant 2x_1\ (x_1<0,x_1+x_2+x_3+x_4+x_5\geqslant 1)\\&\leqslant -2\ (\text{由 } x_1<0 \text{ 且 } x_1\in\mathbf{Z} \text{ 知 } x_1\leqslant -1).\end{aligned}$$

即每操作一次后，f 的值至少下降 2，又由于 f 非负，所以上述操作不能无限地进行下去.

所以这样的操作进行有限次后必定终止.

评注 本题所构造的函数并不唯一，例如可构造辅助函数 $g(x_1,x_2,x_3,x_4,x_5)=\sum\limits_{i=1}^{5}|x_i|+\sum\limits_{i=1}^{5}|x_i+x_{i+1}|+\sum\limits_{i=1}^{5}|x_i+x_{i+1}+x_{i+2}|+\sum\limits_{i=1}^{5}|x_i+x_{i+1}+x_{i+2}+x_{i+3}|$（这里认为 $x_{n+5}=x_n$），也能解决问题，有兴趣的读者不妨亲自验证一下.

例 3 在坐标平面上，如果点 (x_0,y_0) 的坐标 x_0,y_0 都是整数，那么称该点为整点，试证：在坐标平面上，不存在正 n 边形（$n\geqslant 7$），使其各顶点都是整点.

证明 假设存在某个正 n 边形 $A_1A_2A_3\cdots A_n$（$n\geqslant 7$），其各顶点 $A_1,A_2,\cdots,A_n$ 都是整

点.

在坐标平面内任取一整点 M，过 M 点分别作向量$\overrightarrow{MB_1}$，$\overrightarrow{MB_2}$，$\overrightarrow{MB_3}$，…，$\overrightarrow{MB_n}$使得$\overrightarrow{MB_1}=\overrightarrow{A_1A_2}$，$\overrightarrow{MB_2}=\overrightarrow{A_2A_3}$，$\overrightarrow{MB_3}=\overrightarrow{A_3A_4}$，…，$\overrightarrow{MB_{n-1}}=\overrightarrow{A_{n-1}A_n}$，$\overrightarrow{MB_n}=\overrightarrow{A_nA_1}$（如图 6－1）.

因为 $A_1,A_2,\cdots,A_n,M$ 都是整点，则由向量的坐标运算可以得知 $B_1,B_2,\cdots,B_n$ 都是整点.

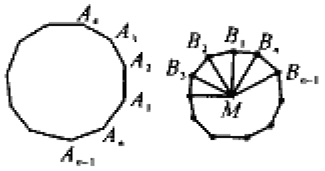


图 6-1

又易知$|\overrightarrow{MB_i}|=|\overrightarrow{MB_{i+1}}|$（$i=1,2,\cdots,n$，定义 $B_{n+1}=B_1$），且$\overrightarrow{MB_i}$与$\overrightarrow{MB_{i+1}}$间的夹角为$\frac{2\pi}{n}$.

所以 n 边形 $B_1B_2\cdots B_n$ 是正 n 边形.

则易知 n 边形 $B_1B_2\cdots B_n$ 与 n 边形 $A_1A_2\cdots A_n$ 相似，相似比即为$\frac{|B_1B_2|}{|A_1A_2|}=\frac{|B_1B_2|}{|MB_1|}$，而$\angle B_1MB_2=\frac{2\pi}{n}$，则$\frac{|B_1B_2|}{|MB_1|}=2\cos\frac{\pi}{n}$.

所以 $B_1B_2=2\cos\frac{\pi}{n}\cdot|A_1A_2|\leqslant 2\cos\frac{\pi}{7}|A_1A_2|$.

上述这一过程可以无限地进行下去，即由原正 n 边形可以得到一系列正 n 边形，每个正 n 边形边长都不大于前一个正 n 边形边长的 $2\cos\frac{\pi}{7}$，即对任意 $m\in\mathbf{N}_+$，都存在一个顶点都是整点的凸 n 边形，其边长不大于$\left(2\cos\frac{\pi}{7}\right)^m\cdot|A_1A_2|$，但 $2\cos\frac{\pi}{7}<1$，则当 $m\to+\infty$时，$\left(2\cos\frac{\pi}{7}\right)^m\cdot|A_1A_2|\to 0$，而任两个不同整点间的距离至少为 1，即正 n 边形边长不小于 1，这就导致了矛盾.

所以，不存在正 n 边形（$n\geqslant 7$），使其各顶点都是整点.

例 4 假设 $2n+1$ 个正整数 $a_1,a_2,\cdots,a_{2n+1}$ 有这样的性质：任取其中 $2n$ 个数，总可以分为两个无公共元素的 n 元子集，且两个子集中 n 个数的和相等，那么这 $2n+1$ 个数必全相等.

证明 如果有 $2n+1$ 个正整数满足题中所述性质，我们则称这 $2n+1$ 个正整数为“好数组”，不妨设 $a_1\leqslant a_2\leqslant\cdots\leqslant a_{2n+1}$，并且 $a_1=1$（因为把最小数减少至 1，其余数都减去与之相同的一个数，所得到的一组新数仍为“好数组”.）

又依题设可知 $2\left|\left(\left(\sum\limits_{i=1}^{2n+1}a_i\right)-a_j\right)\right.$（$j=1,2,3,\cdots,2n+1$），即 $a_1\equiv a_2\equiv a_3\equiv a_4\equiv\cdots\equiv a_{2n+1}\equiv\sum\limits_{i=1}^{2n+1}a_i\pmod 2$.

由于 $a_1=1$，所以 $a_1,a_2,a_3,\cdots,a_{2n+1}$ 均为正奇数.

令 $b_i=\frac{a_i+1}{2}(i=1,2,\cdots,2n+1)$，由于 $a_1,a_2,\cdots,a_{2n+1}$ 均为正奇数，所以 $b_1,b_2,b_3,\cdots,b_{2n-1}$ 均为正整数且易知 $b_1,b_2,b_3,\cdots,b_{2n+1}$ 也是"好数组".

因为当 $x<y$ 时，$\frac{x+1}{2}<\frac{y+1}{2}$，

所以 $b_1\leqslant b_2\leqslant\cdots\leqslant b_{2n+1}$.

如果 $a_{2n+1}>1$，则 $b_{2n+1}=\frac{a_{2n+1}+1}{2}<a_{2n-1}$，反复进行上述变换，最终必得到一个"好数组"，其最大项为1，又在上述变换中每个数组最小项均为1，所以这"好数组"中各项均为1.再考虑上述变换的方式(将 x 变为$\frac{x+1}{2}$)即可知最初的 $2n+1$ 个数 $a_1,a_2,\cdots,a_{2n+1}$ 均为1.

由此就证明了原命题.

评注 事实上，如果 $2n+1$ 个有理数 $x_1,x_2,\cdots,x_{2n+1}$ 满足：从中任取 $2n$ 个数，总可以分成两个无公共元素的 n 元子集，且两个子集中 n 个数的和相等，我们同样可以证明这 $2n+1$ 个有理数相等，只需将本题的证明稍加改进即可，有兴趣的读者不妨一试.

例5 设 $f(x)=x^2+x+p,p\in\mathbf{N}$，求证：如果 $f(0),f(1),f(2),\cdots,f\left(\left[\sqrt{\frac{p}{3}}\right]\right)$ 是素数，那么数 $f(0),f(1),\cdots,f(p-2)$ 都是素数.

分析 如果存在某个 $m\in\{0,1,2,\cdots,p-2\}$，使 m^2+m+p 为合数，而我们又能通过某种方式使 m 下降，即找到一个比 m 更小的数 $m'(m'\in\{0,1,2,\cdots,p-2\})$，使 $f(m')$ 为合数，则由无穷递降法就可以导出矛盾.

证明 当 $0\leqslant x\leqslant p-2$ 时，$p\leqslant x^2+x+p\leqslant(p-2)^2+(p-2)+p=(p-1)^2+1$.

设 x_0 是使 $f(x)=x^2+x+p$ 为合数的最小的自然数 x 的值.

若 $0\leqslant x_0\leqslant p-2$，则 $x_0^2+x_0+p\leqslant(p-1)^2+1$，

从而 $x_0^2+x_0+p$ 的最小素因子 $d_0\leqslant p-1$.

设 $x_0^2+x_0+p=d_0m(m\in\mathbf{N}_+)$.

(1)如果 $x_0\geqslant d_0$，令 $x'=x_0-d_0$，

$$\begin{aligned}\text{则有 } x'^2+x'+p&=(x_0-d_0)^2+(x_0-d_0)+p\\&=x_0^2+x_0+p-d_0(2x_0-d_0+1)\\&=d_0(m-2x_0+d_0-1),\end{aligned}$$

由于 $x'^2+x'+p\geqslant p>p-1\geqslant d_0$，所以 $m-2x_0+d_0-1>1$.

从而可以得知 $d_0(m-2x_0+d_0-1)$ 为合数，即 $f(x')$ 为合数，且 $0\leqslant x'=x_0-d<x_0$，这就与 x_0 的定义相矛盾.

(2)如果 $x_0<d_0$，令 $x'=d_0-1-x_0$，

则有 $x'^2+x'+p=(d_0-1-x_0)^2+(d_0-1-x_0)+p$

$=x_0^2+x_0+p-d_0(2x_0-d_0+1)$

$=d_0(m-2x_0+d_0-1)$，

与(1)中的方法相同，我们可以证明 $f(x')$ 为合数，则由 x_0 的定义知 $x'\geqslant x_0$，

即 $d_0-1-x_0\geqslant x_0$，从而 $d_0\geqslant 2x_0+1$，

又 $d_0\leqslant\sqrt{f(x_0)}$($d_0$ 为合数 $f(x_0)$ 的最小素因子)，

所以 $2x_0+1\leqslant d_0\leqslant\sqrt{f(x_0)}$.

即 $4x_0^2+4x_0+1\leqslant x_0^2+x_0+p$，

解之得 $\frac{-3-\sqrt{12p-3}}{6}\leqslant x_0\leqslant\frac{-3+\sqrt{12p-3}}{6}$.

因 $\frac{-3+\sqrt{12p-3}}{6}=-\frac{1}{2}+\sqrt{\frac{p}{3}-\frac{1}{12}}<\sqrt{\frac{p}{3}}$.

所以 $0\leqslant x_0\leqslant\left[\sqrt{\frac{p}{3}}\right]$.

而由题中条件知 $f(0),f(1),\cdots,f\left(\left[\sqrt{\frac{p}{3}}\right]\right)$ 均为素数，但 $f(x_0)$ 为合数，矛盾!

所以必有 $x_0>p-2$，则由 x_0 的定义可知 $f(1),f(2),\cdots,f(p-2)$ 都是素数.

原命题得证.

评注 在上述证明过程中，我们似乎并未用到无穷递降法，这是因为在开始我们采用了“走极端”的方法.通常为便于叙述，我们都会采取这种方法(但这种方法并不总是可行的)，将无穷递降的过程压缩到一步递降，从而达到简化证明的目的.

例 6 (2006 年国家集训队测试题)求所有的正整数对 (a,n) 使得 $\frac{(a+1)^n-a^n}{n}$ 是整数.

解 首先指出 $(a,1)$ 显然是原问题的解(这里 a 为任意正整数)，下面我们证明原问题没有其他解.

假设 $(a,n)(n\geqslant 2)$ 是原问题的一个解，则必存在正整数 k，使得 $(a+1)^n-a^n=kn$.

由于 $a+1$ 与 a 互素，则由上式可知 n 与 a 和 $a+1$ 都互素，则由欧拉定理可得:

$(a+1)^{\varphi(n)}\equiv a^{\varphi(n)}\equiv 1(\bmod n)$.

设 $d=(n,\varphi(n))$，则由 Bezout 定理知存在整数 α 和 β 使得

$d=\alpha n+\beta\varphi(n)$，

由 $(a+1)^n\equiv a^n(\bmod n)$ 及 $(a+1)^{\varphi(n)}\equiv a^{\varphi(n)}\equiv 1(\bmod n)$(由 $(a+1)^n-a^n=kn$，可知 $(a+1)^n\equiv a^n(\bmod n)$)，可以推出

$(a+1)^d \equiv (a+1)^{sn+t\varphi(n)} \equiv a^{sn+t\varphi(n)} \equiv a^d \pmod{n}$. ①

显然 $d>1$（否则 $a+1\equiv a \pmod{n}$，则 $n=1$，与假设不符），同时注意到 $\varphi(n)<n$.

所以 $1<d<n$.

又 $n \mid ((a+1)^d-a^d)$（这是因为①式）且 $d \mid n$，故 $d \mid ((a+1)^d-a^d)$.

于是我们又找到原问题的另一个解 (a,d) 并且 $1<d<n$.

重复上述过程我们就得到从 n 开始的一个无穷递降的正整数列，显然这是不可能的.

因此先前的假设有错误，即没有 $n>1$ 的解.

所以，使得 $\dfrac{(a+1)^n-a^n}{n}$ 是整数的所有正整数对 (a,n) 即为 $(a,1)$（其中 a 可取任意正整数）.

例 7 在平面上给出了有限条红色直线和蓝色直线，其中任何两条不平行，并且其中任何两条同色直线的交点处都有一条与它们异色的直线经过，证明：所有给定的直线都交于一点.

证明 假设所有给定直线不相交于一点.

对于所定的直线中的任一条红线 l，设它与各条蓝色直线交于 $A_1, A_2, \cdots, A_n$，不妨设这 n 个点中 A_1 与 A_n 距离最大（若 A_1 与 A_n 重合，则题中所要证明的结论显然成立，这里假设 A_1 与 A_n 不重合），设与 l 交于 A_1, A_n 的两条蓝色直线交于 B，这样构成一个三角形 $\triangle A_1A_nB$.

依题意，必有一条红色直线 l' 过点 B，设 l' 与 l 交于 C，我们现在来证明点 C 在线段 A_1A_n 上.

若点 C 不在线段 A_1A_n 上，如图 6-2，不妨设点 C 在 A_nA_1 的延长线上（点 C 必不与 A_1, A_n 重合），则依题意知存在一条过 C 的蓝色直线，则点 C 也是 l 与某条蓝色直线的交点，而 $CA_n>A_1A_n$，这就与 A_1A_n 的最大性矛盾.

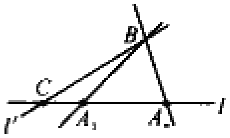


图 6-2

所以点 C 必在线段 A_1A_n 上.

于是，我们由一条红线 l 便得到一个“四线组”（例如直线 l, BC, BA_1, BA_n），并称由这条直线所围成的三角形中面积最大的三角形的面积为这个“四线组”的“质量”.

同理，对任意一条蓝线，我们也可以类似地得到一个“四线组”，用同样的方式对其定义“质量”.

这样一来，对任意一给定的直线，我们都可以得到一个“四线组”，从中任取一个，如图 6-3，不妨设 l_1, l_2 为蓝线，l_3, l_4 为红线，设 $P=l_2\cap l_1\cap l_4$，$Q=l_2\cap l_3$，$R=l_3\cap l_4$，$S=l_1\cap l_3$.

由题意知，必有一条蓝色直线过 R，则该直线必与线段 PQ 及线段 PS 之一相交，不妨该蓝色直线与线段 PS 交于 T，则直线 PS, PR, RT, RS 又组成一个“四线组”（直线

PS,RT 为蓝色，直线 PR,RS 为红色），而“四线组”(PS,PR,RT,RS) 的“质量”为 $S_{\triangle RQS}$，“四线组”(l_1,l_2,l_3,l_4) 的“质量”为 $S_{\triangle PQS}>S_{\triangle RQS}$. 即我们由原“四线组”得到了一个新“四线组”且新“四线组”的“质量”小于原“四线组”的“质量”.

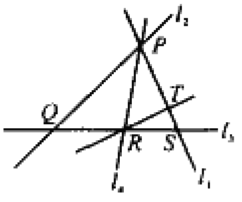


图 6-3

将上述过程不断地进行下去，则所得“四线组”的“质量”不断地减小，而“四线组”的个数是有限的. 这就导致了矛盾. 所以假设是错误的.

故所有给定直线交于一点.

评注 本题前半部分对“四线组”存在性的证明极易让人误以为 A_1A_n 的最大性也是“四线组”的定义之一，事实上并非如此，如图 6-3，只需直线 l_1 与 l_2 同色且与 l_3，l_4 异色，即可称 l_1,l_2,l_3,l_4 为一个“四线组”，而并不要求 Q,S 一定是 l_3 与跟它异色的直线的交点中距离最远的两点.

例 8 （第 29 届俄罗斯数学奥林匹克）正整数序列 $\{a_n\}$ 按如下方式构成：a_0 为某个正整数，如果 a_n 可以被 5 整除，则 $a_{n+1}=\frac{a_n}{5}$；如果 a_n 不能被 5 整除，则 $a_{n+1}=[\sqrt{5}a_n]$（其中 $[x]$ 表示不超过 x 的最大整数）. 证明：数列 $\{a_n\}$ 自某一项开始递增.

证明 首先指出对于任意正整数 x，都有 $[\sqrt{5}x]\geqslant x+1$.

这是因为当 $x\in\mathbf{N}_+$ 时，$\sqrt{5}x>2x\geqslant x+1$.

所以 $[\sqrt{5}x]\geqslant[x+1]=x+1$.

由此我们可以得知题中所要证明的结论等价于：存在某个正整数 m，使对一切 $n\geqslant m$，$n\in\mathbf{N}_+$，a_n 都不是 5 的倍数（此时 $a_{n+1}=[\sqrt{5}a_n]>a_n$），下面我们便来证明这一点.

为此，我们首先证明数列 $\{a_n\}$ 中存在两个相邻的项都不是 5 的倍数.

用反证法来证明，假设数列 $\{a_n\}$ 中任两个相邻的项中都至少有一个是 5 的倍数. ①

考察 a_1,a_2,a_3.

(1) 如果 $5\mid a_1$，则 $a_2=\frac{a_1}{5}$，又由 $\{a_n\}$ 的递推式可以得知 $a_3\leqslant[\sqrt{5}a_2]$，于是 $a_3\leqslant\left[\frac{\sqrt{5}}{5}a_1\right]<a_1$.（由于 $a_2=\frac{a_1}{5}$ 为正整数，故有 $5\cdot\frac{a_1}{5}>\sqrt{5}\cdot\frac{a_1}{5}\geqslant\left[\frac{\sqrt{5}}{5}a_1\right]$），即有 $a_3\leqslant a_1-1$.

(2) 如果 $5\nmid a_1$，则由①中假设知 $5\mid a_2$，于是有 $a_2=[\sqrt{5}a_1]$，$a_3=\frac{a_2}{5}$，所以 $a_3=\frac{[\sqrt{5}a_1]}{5}<a_1$，即有 $a_3\leqslant a_1-1$.

综合(1)，(2)即知，无论哪种情况都有 $a_3\leqslant a_1-1$，即我们从 a_1 开始可以找到数列 $\{a_n\}$ 中的一项 a_3，使得 $a_3\leqslant a_1-1$，同样地，我们从 a_3 开始可以找到数列 $\{a_n\}$ 中的一项 a_5，使得 $a_5\leqslant a_3-1$，……，将这一过程不断地进行下去，每次找出的新项都至少比它的原

项小 1，而数列$\{a_n\}$中各项都为正整数，故这一过程应不能无限进行下去，由此得出矛盾.

所以①中假设不成立.

从而，我们证明了数列$\{a_n\}$中必存在两个相邻项都不是 5 的倍数.

于是，我们可以找出相邻两项 a_k 和 a_{k+1} 都不是 5 的倍数.

我们再来证明一个引理：

引理：若 a_n 和 a_{n+1} 都不是 5 的倍数，则 a_{n+2} 也不是 5 的倍数.

引理的证明：由于 a_n 不是 5 的倍数，那么由题意可得

$a_{n+1}=[\sqrt{5}a_n]$，$a_{n+2}=[\sqrt{5}a_{n+1}]$.

设 $a_{n+1}=\sqrt{5}a_n-\alpha$，其中 $0<\alpha\leq 1$.

则 $a_{n+2}=[\sqrt{5}a_{n+1}]=[\sqrt{5}(\sqrt{5}a_n-\alpha)]=5a_n+[-\sqrt{5}\alpha]$.

由于 $0<\alpha<1$，

所以 $-3<-\sqrt{5}\alpha<0$，那么$[-\sqrt{5}\alpha]=-3$ 或 -2 或 -1.

故 $a_{n+2}=[-\sqrt{5}\alpha]\equiv -3$ 或 -2 或 $-1 \pmod 5$.

因此 a_{n+2}不是 5 的倍数，引理得证.

利用引理及 a_k 和 a_{k-1} 都不是 5 的倍数，我们就可以得知：当 $n\geq k$ 时，a_n 不是 5 的倍数，再结合最初的推导，就证明了原命题成立.

能力训练

1. 证明$\sqrt{5}$是无理数.

2. 平面上给定 $2n$ 个点，没有三点共线，n 个点代表农场 $F=\{F_1,F_2,\cdots,F_n\}$，另 n 个点代表水库 $W=\{W_1,W_2,\cdots,W_n\}$，一个农场与一个水库用直路相连接. 证明存在一种分配方式，使得所有的路不相交.

3. 设 M 是平面上的有限点集. 已知过 M 中任何两点所作的直线必过 M 中另一点，求证：M 中所有的点共线.

4. 在平面上给出某个点集 M，使得 M 中每个点都是集合 M 中某两点连结线段的中点，证明：集合 M 中一定包含无穷多个点.

5. 设有 $2n$ 个整数 $a_1,a_2,\cdots,a_{2n}$，在其中任意取出一个数，其余的 $2n-1$ 个数总可以分为两个无公共元素的子集，使每个子集中各数之和相等，那么 $a_1,a_2,\cdots,a_{2n}$必全为零.（这里的“两个无公共元素的子集”指的是对余下的任一个 a_i，它恰属于一个子集）.

6. 证明：勾股三角形的面积不可能为一个完全平方数.

第七章 格点及其性质

§7.1 格点的定义及分类

知识扫描

1. 格点的定义 在平面直角坐标系中，横、纵坐标都是整数的点叫做格点(整点).

2. 格点的分类 根据整数的奇偶性可以把格点分为(奇，奇)、(奇，偶)、(偶，奇)、(偶，偶)四类.一线段的两端点，如果是同一类型的格点，那么这条线段的中点也是格点，反之亦然.

事实上，格点的定义还能推广到空间直角坐标系中，格点的分类也远远不止奇偶分类一种，其他的分类方法在下面的例题当中再作分析.

例题分析

例 1 对任意正整数 n，连结原点 O 和点 $A_n(n,n+3)$. 用 $f(n)$ 表示线段 OA_n 上除端点外的格点的个数，求 $f(1)+f(2)+\cdots+f(2006)$.

解 线段 OA_n 的方程为 $y=\frac{n+3}{n}x\,(0\leqslant x\leqslant n)$，则 $f(n)$ 就是方程 $y=\frac{n+3}{n}x$ 在 $(0,n)$ 内的整数解的个数.

我们可以把格点 A_n 分成两类：第 1 类是横、纵坐标互质的格点，第 2 类是横、纵坐标不互质的格点，当 A_n 是第一类格点时，$(n,n+3)=1$，则方程 $y=\frac{n+3}{n}x$ 在 $(0,n)$ 内无整数解；当 A_n 是第二类格点时，$(n,n+3)=1$，则 $3\mid n$，设 $n=3k(k\in\mathbf{N}_+)$，则方程变形为 $y=\frac{k+1}{k}x(0<x<3k)$，有两个整数解.

所以，$f(1)+f(2)+\cdots+f(2006)$ 表示 $A_1,A_2,\cdots,A_{2006}$ 中第二类格点个数的两倍，等于 $2\cdot\left[\frac{2006}{3}\right]=1336$.

例 2 空间中有一凸多面体，它的所有顶点都是格点（每个顶点的三个坐标值都是整数），此外，在多面体的内部，面上和棱上都不再有其他整点.问这个凸多面体顶点个数的最大值是多少.

分析与解 首先，我们取坐标为 $(i,j,k)(i,j,k\in\{0,1\})$ 的八个格点，以这 8 个格点为顶点可以得到一个单位立方体，而这个单位立方体显然满足题设要求，故所求的最小值不小于 8. 另一方面，每个格点的三个坐标按奇偶性可以分为如下八类：

（奇，奇，奇）、（奇，奇，偶）、（奇，偶，奇）、（奇，偶，偶），

（偶，奇，奇）、（偶，奇，偶），（偶，偶，奇），（偶，偶，偶）.

如果这个多面体有 9 个顶点，由抽屉原则，必有两个顶点属于同一类格点，则这两个顶点连线的中点也是格点，由多面体的凸性知，该格点属于这个多面体，与已知矛盾. 故所求的顶点个数不大于 8.

综上，该凸多面体最多有 8 个顶点.

评析 将格点按照恰当方式分类后，能够使格点与格点之间的联系趋于明显，将格点按坐标的奇偶性分类是研究图形中两格点连线上的格点问题的重要手段.

例 3 （2004 年克罗地亚数学竞赛题）一只青蛙在平面直角坐标系上从点 $(1,1)$ 开始按照如下规则跳跃：(1)该青蛙能从任一点 (a,b) 跳到点 $(2a,b)$ 或 $(a,2b)$；(2)如果 $a>b$，该青蛙能从 (a,b) 跳到 $(a-b,b)$，如果 $a<b$，该青蛙能从 (a,b) 跳到 $(a,b-a)$.

问：这只青蛙能到达点①$(24,40)$，②$(40,60)$，③$(24,60)$，④$(200,4)$吗？

分析 不论按规则(1)还是按规则(2)跳跃，青蛙所能到达的格点的两个坐标值的公共奇因子保持不变.

解 对①、④，答案是肯定的，我们给出青蛙从点 $(1,1)$ 到给定点的路径实例：

①的路径是

$(1,1)\to(2,1)\to(4,1)\to(3,1)\to(3,2)\to(3,4)\to(3,8)\to(3,5)\to(6,5)$

$\to(12,5)\to(24,5)\to(24,10)\to(24,20)\to(24,40)$.

④的路径是

$(1,1)\to(2,1)\to(4,1)\to(8,1)\to(16,1)\to\cdots\to(64,1)\to(63,1)\to(62,1)$
$\to(61,1)\to(60,1)\to\cdots\to(50,1)\to(50,2)\to(50,4)\to(100,4)\to(200,4)$.

对于②、③，答案是否定的，用规则(1)和规则(2)都不能到达 x 和 y 有公共奇因子(大于 1)的点(x,y). 而 40 和 60 都能被 5 整除，24 和 60 都能被 3 整除，因此，青蛙从点(1,1)出发不能到达(40,60)和(24,60).

例 4 请设计一种方法将所有的整点染色，每点染成白色、红色或黑色中的一种颜色，使得：(1)每种颜色的点都出现在无穷多条平行于横轴的直线上.

(2)使得任意的白点 A，红点 B，黑点 C，总可以找到一个红点 D，使得 $ABCD$ 是一个平行四边形.

分析 根据格点的分类来染色，使条件(1)成立，让 A、B、C 各点数量化(标上坐标)，根据平行四边形对角线互相平分及中点坐标公式求出 D 的坐标，应能得到满足条件(2)的平行四边形 $ABCD$.

解 设计如下的染色方法：把(奇、奇)类格点染成白色，(偶，偶)类格点染成黑色，(奇，偶)和(偶，奇)类格点染成红色，易知这种染色方法满足条件(1).

任取白点 $A(2m+1,2n+1)$，黑点 $C(2s,2t)$，红点 $B(2p,2q+1)$，其中 m,n,s,t,p,q 均为整数，再设平行四边形 $ABCD$ 的顶点 D 的坐标为(x,y).

由平行四边形对角线互相平分及中点坐标公式得

$$\begin{cases}x+2p=2m+1+2s,\\ y+2q+1=2n+1+2t.\end{cases}$$

解出 $x=2m+1+2s-2p$，$y=2(n+t-q)$.

由此可得 $D(x,y)$是(奇，偶)类格点，所染的色也是红色.

同理，若点 B 是(奇，偶)类格点，可推得 D 是(偶，奇)类格点，所染的色也是红色，故这样的设计方案也满足(2).

例 5 任取 6 个格点 $p_i(x_i,y_i)(i=1,2,3,4,5,6)$，满足

(1) $|x_i|\leqslant 2$，$|y_i|\leqslant 2(i=1,2,3,4,5,6)$；

(2)任何三点都不在同一直线上.

试证：在以 $p_i(i=1,2,3,4,5,6)$为顶点的所有三角形中，必有一个三角形，它的面积不大于 2.

证明 假设存在 6 个格点 $p_1,p_2,\cdots,p_6$ 落在区域 $S=\{(x,y)\mid |x|\leqslant 2,|y|\leqslant 2\}$内，它们任 3 个点所成的三角形面积都大于 2，记 $p=\{p_1,p_2,\cdots,p_6\}$.

(1)若 x 轴具有 p 中的点数小于 2，则由抽屉原则，x 轴的上半平面(或下半平面，不包含 x 轴)至少有 p 的 3 个点. 此 3 点所成的三角形面积不大于 2，矛盾. 故 x 轴上恰有 p 的 2 个点(因不能有 3 点共线)，又剩下 p 中的 4 个点不可能有一点在直线 $y=\pm 1$ 上，否

则出现以 p 中的点为顶点的面积不大于 2 的三角形，这就证明了，在直线 $y=2$ 和 $y=-2$ 上，都恰有 p 的两个点. 注意到 S 的对称性，同理可证：直线 $x=-2, x=0, x=2$ 上分别有 p 中的两个点，于是，在每条直线 $y=2j, x=2j(j=0,\pm1)$ 上恰有 p 的两个点.

(2) p 必不能包含原点，否则，因 S 内纵、横坐标均为偶数的所有格点落在且仅落在过原点的 4 条直线上，由抽屉原则，剩下的 p 的 5 个点，至少有两点落在这些直线的一条上，于是 3 点共线，矛盾.

因此，p 中在 x 轴的两点必是 $(-2,0),(2,0)$，同理，在 y 轴上的两点必是 $(0,2)$ 和 $(0,-2)$，另外的两点只能取 $(-2,-2),(2,2)$ 或 $(-2,2),(2,-2)$. 不论哪一种情形，都得到一个以 p 的点为顶点的面积不大于 2 的三角形，矛盾.

能力训练

1. 无论形状如何，使格点凸 n 边形内部及边界上格点总个数 $\geqslant n+1$ 的最小正整数 n 等于(　　)

A. 4　　B. 5　　C. 6　　D. 7

2. 在平面上所有过点 $\left(10,\frac{1}{2}\right)$ 的直线中，至少经过两个格点的直线的条数有(　　)

A. 一条　　B. 不存在

C. 有限条但不少于 2 条　　D. 无穷多条

3. 已知直线 l 的方程为 $y=\frac{5}{3}x+\frac{4}{5}$，则与 l 距离最近的格点到 l 的距离等于(　　)

A. $\frac{\sqrt{34}}{85}$　　B. $\frac{\sqrt{34}}{170}$　　C. $\frac{3\sqrt{34}}{170}$　　D. $\frac{2\sqrt{34}}{85}$

4. C 是半径为 r 的圆，圆心在点 $(\sqrt{2},\sqrt{3})$，r 是正实数，则 C 上整点个数最多有(　　)个.

A. 0　　B. 1　　C. 4　　D. 无穷

5. 在直角坐标系中，将格点按以下方法编号：$(0,0)$ 是第 1 号，$(1,0)$ 是第 2 号，$(1,1)$ 是第 3 号，$(0,1)$ 是第 4 号，$(0,2)$ 是第 5 号，$(1,2)$ 是第 6 号，$(2,2)$ 是第 7 号，$(2,1)$ 是第 8 号，$(2,0)$ 是第 9 号，…(如图 7-1). 按图中箭头顺序，第 2006 号点的坐标是________.

6. 在直角坐标系中，满足 $(|x|-1)^2+(|y|-1)^2<2$ 的整点 (x,y) 有________个.

7. 已知点集 $A=\left\{(x,y)\mid(x-3)^2+(y-4)^2\leqslant\left(\frac{5}{2}\right)^2\right\}$，$B=\{(x,y)\mid(x-4)^2+(y-

5)$^2>\left(\frac{5}{2}\right)^2$}，则 $A\cap B$ 中整点的个数为________.

8. 设 T 是平面中所有格点的集合，对于整点 (x,y) 与 (u,v)，当且仅当 $|x-u|+|y-v|=1$ 时，称为相邻的点. 求证：存在 T 的一个子集 S，使得对于每一个点 $P\in T$，在 P 与 P 的相邻点中恰有一个属于 S.

9. 若三角形的顶点都是格点，其周界上没有其他的格点，在它内部恰有一个格点，证明这个格点为三角形的重心.

10. 求证：平面上存在一个无限整点集 T，T 中任意三点不共线，且 T 中每两个元素的距离都为无理数.

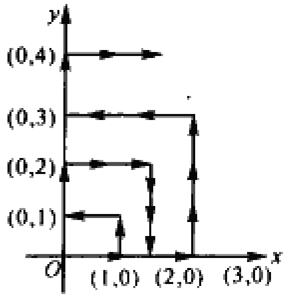


图 7-1

§7.2 格点的计数

知识扫描

一个区域内或一条曲线上格点个数的计算问题，常常采用观察法、归纳法、整除法、格点多边形面积等方法求得.

格点多边形是指顶点都是格点的多边形，一个格点多边形的内部有 N 个格点，边界上有 L 个格点，则此格点多边形的面积为 $S=N+\frac{1}{2}L-1$.

定理 (1)设函数 $f(x)$ 在闭区间 $[a,b]$ 上连续且非负(如图 7-2 所示)，则和式 $\sum\limits_{a<t\leqslant b}[f(t)]$ 表示平面区域 $a<x\leqslant b$，$0<y\leqslant f(x)$ 内的格点的个数，其中 t 表示 $(a,b]$ 中的整数，$[f(t)]$ 表示 $f(t)$ 的高斯函数.

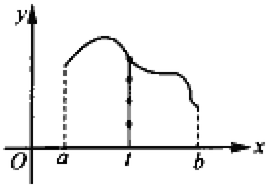


图7-2

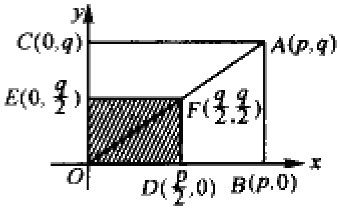


图7-3

(2)设正整数 p,q 满足 $(p,q)=1$，则

$$\sum_{0<x<\frac{p}{2}}\left[\frac{q}{p}x\right]+\sum_{0<y<\frac{q}{2}}\left[\frac{p}{q}y\right]=\left[\frac{p-1}{2}\right]\cdot\left[\frac{q-1}{2}\right].$$

其证明如下：如图 7-3 所示，因为 $(p,q)=1$，所以线段 OF 上除 O 外再无格点，则 $\sum\limits_{0<x<\frac{p}{2}}\left[\frac{q}{p}x\right]$ 表示 $\triangle ODF$ 内的格点的个数，$\sum\limits_{0<y<\frac{q}{2}}\left[\frac{p}{q}y\right]$ 表示 $\triangle OEF$ 内格点的个数，因此 $\sum\limits_{0<x<\frac{p}{2}}\left[\frac{q}{p}x\right]+\sum\limits_{0<y<\frac{q}{2}}\left[\frac{q}{p}y\right]$ 表示长方形 $ODFE$ 内的格点个数，这在数值上等于 $\left[\frac{p-1}{2}\right]\cdot\left[\frac{q-1}{2}\right]$.

格点计数问题不限于是简单地数格点的个数，在本讲中，我们还会涉及有关格点多边形的一些问题.

例题分析

例 1 直线 $y=x$ 和抛物线 $y=2^{-100}x^2$ 所围的图形为 F，则在图形 F 内（不包括边界）坐标形如 $(2^m,2^n)$ 的点的个数有多少个 $(m,n\in\mathbf{N}_+)$.

解 $y=x$ 与 $y=2^{-100}x^2$ 交于 $(0,0)$ 和 $(2^{100},2^{100})$，点 $(2^m,2^n)$ 应满足 $0<m<100$，$m>n>2m-100$，当 $m=k(2\leqslant k\leqslant 50)$ 时，n 可取 $1,2,\cdots,k-1$，当 $m=k(51\leqslant k\leqslant 99)$ 时，n 可取 $2k-99,2k-98,\cdots,k-1$，所以共有

$$\sum_{k=2}^{50}(k-1)+\sum_{k=51}^{99}(99-k)=\frac{50\times 49}{2}+\frac{49\times 48}{2}$$

$=2401$ 个形如 $(2^m,2^n)$ 的格点 $(m,n\in\mathbf{N}_+)$.

例 2 设 $\triangle ABC$ 是格点三角形，且在 $\triangle ABC$ 的内部只有一个整点（但在边界上允许有整点）. 求证：$\triangle ABC$ 的面积 $\leqslant\frac{9}{2}$.

证明 设 O 为 $\triangle ABC$ 内的整点，BC、CA、AB 边的中点分别为 A_1，B_1，C_1.

显然，O 或在 $\triangle A_1B_1C_1$ 内部或在 $\triangle A_1B_1C_1$ 的边界上.

否则，由于 A，B，C 关于 O 点的对称点均为整点，则在 $\triangle ABC$ 内就不止一个整点.

不妨设点 O 不在线段 A_1B_1 上或线段 A_1C_1 上.

设 A_2 是点 A 关于点 O 的对称点，D 是平行四边形 $ABDC$ 的第四个顶点，则 A_2 为 $\triangle BCD$ 的内点或在它的边界上.

(1)若 A_2 是 $\triangle BCD$ 的内点.

因为 A_2 是整点，所以 A_2 就是 O 关于平行四边形 $ABDC$ 中心 A_1 的对称点——

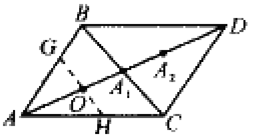


图 7-4

$\triangle BCD$ 内唯一的整点 A、O、A_2 和 D 是线段 AD 上相继的整点，所以 $AD=3AO$.

由于 A、B、C 地位作用相同，所以 O 是 $\triangle ABC$ 的重心，过 O 作线段 $GH\parallel BC$，若 BC 内部的整点多于两个，则 GH 内部必含有一个不同于 O 的整点(这是因为 BC 上每两个相邻整点的距离 $\leqslant\frac{1}{4}BC$，而 $OG=OH=\frac{1}{3}BC$)，出现矛盾. 因此 BC 的内部至多只有两个整点，AB 与 AC 有同样的结论.

总之，在 $\triangle ABC$ 的周界上的整点数 $\leqslant 9$，则由格点多边形的面积计算定理知

$\triangle ABC$ 的面积 $\leqslant 1+\frac{9}{2}-1=\frac{9}{2}$.

(2)若 A_2 在 $\triangle BCD$ 的边界上.

与(1)类似，可以推出 BC 边内部的整点数不超过 3(仅当 O 在 B_1C_1 上时，出现 3 个整点). AB 与 AC 内部的整点数均不多于 1.

总之，$\triangle ABC$ 周界上的整点数 $\leqslant 8$，因此

$\triangle ABC$ 的面积 $\leqslant 1+\frac{8}{2}-1=4$.

由(1)，(2)命题得证.

评析 事实上，本题就是一个利用格点多边形的面积定理的问题，于是顺利地将问题由证明 $\triangle ABC$ 面积 $\leqslant\frac{9}{2}$，转变为证明 $\triangle ABC$ 的边界上的整点个数 $\leqslant 9$. 这样就将问题变得简明清晰了，剩下的过程就是利用 O 点为 $\triangle ABC$ 内唯一一个格点的性质，给出 $\triangle ABC$ 边界上点的个数的一个上界.

例 3 直角坐标系中，满足(1) $y\geqslant 3x$；(2) $y\geqslant\frac{1}{3}x$；(3) $x+y\leqslant 100$ 的整点个数有多少个?

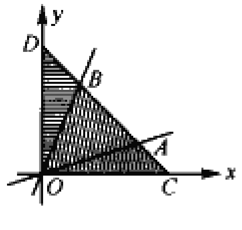


图 7-5

解 如图 7-5 所示，直线 $y=3x$，$y=\frac{1}{3}x$ 及 $x+y=100$ 围成的区域是一个三角形区域，此三角形的三个顶点为 $O(0,0)$，$A(75,25)$，$B(25,75)$.

下面计算 $\triangle OAC$ 的边界及内部的整点个数 N 对 $\triangle OAC$ 的边界或内部的格点 $M(m,n)$. 当 $0\leqslant m<75$ 时，$0\leqslant n\leqslant\frac{1}{3}m$. 当 $75\leqslant m\leqslant 100$ 时，$0\leqslant n\leqslant 100-m$，则

$$N=\sum_{m=0}^{74}\left(\left[\frac{1}{3}m\right]+1\right)+\sum_{m=75}^{100}(100-m+1)$$
$$=\sum_{k=0}^{24}\left(\left[\frac{1}{3}\cdot 3k\right]+1+\left[\frac{1}{3}\cdot(3k+1)\right]+1+\left[\frac{1}{3}\cdot(3k+2)\right]+1\right)+\sum_{m=75}^{100}(100-m+1)$$
$$=\sum_{k=0}^{24}(3k+3)+\sum_{m=75}^{100}(100-m+1)$$
$$=975+351=1326.$$

同理，$\triangle OBD$ 的边界及内部的整点个数也等于 $N=1326$.

而线段 OA 上的整点个数等于 $25+1=26$.

同样地，线段 OB 上有 26 个整点.

设$\triangle OAB$ 内有 L 个整点，则 $L+2N-26\times 2$ 即表示$\triangle OCD$ 内及边界上的所有整点个数，这在数值上就等于 $\sum\limits_{x=1}^{100}([100-x]+1)=\sum\limits_{x=0}^{100}(101-x)=5151$.

所以，$L+2\times 1326-2\times 26=5151$.

故所求的格点个数 $L=2551$.

评注 我们也可以直接从正面计算$\triangle OAB$ 内的整点个数(含边界).

例 4 求证:平面上整点凸五边形的面积不小于$\frac{5}{2}$.

分析 由格点的分类即知格点凸五边形必有两顶点属于同一类，则这两个顶点的连线的中点也是整点，再分此点在凸五边形的边界和内部两类讨论.

证明 考虑整点的纵、横坐标的奇偶性，只有(奇，奇)，(奇，偶)，(偶，奇)，(偶，偶)四类，由抽屉原则，凸五边形 5 个顶点中一定有两个属于同一类型，于是其中点 M 也是整点，由于是凸五边形，故 M 在此五边形的内部或边界上.

(1)若 M 在此凸五边形的内部，此时边界上格点数 $L\geqslant 5$，内部格点数 $N\geqslant 1$，则其面积 $S\geqslant 1+\frac{1}{2}\times 5-1=\frac{5}{2}$.

(2)若 M 在边界上，设 M 在边 P_1P_2 上，因 $P_1P_2P_3P_4P_5$ 是凸五边形，故 P_3P_4 与 P_4P_5 中必有一条与 P_1P_2 不平行. 设 P_3P_4 与 P_1P_2 不平行，于是$\triangle P_2P_3P_4$，$\triangle MP_3P_4$，$\triangle P_1P_3P_4$ 的面积互不相同，则其中最大的一个$\geqslant\frac{3}{2}$，不妨设$\triangle P_1P_3P_4$ 的面积$\geqslant\frac{3}{2}$，而$\triangle P_1P_2P_3$ 与$\triangle P_1P_5P_4$ 都是格点三角形，所以 $S_{\triangle P_1P_2P_3}\geqslant\frac{1}{2}$，$S_{\triangle P_1P_5P_4}\geqslant\frac{1}{2}$，所以，此时凸五边形的面积$\geqslant\frac{3}{2}+\frac{1}{2}+\frac{1}{2}=\frac{5}{2}$.

由(1)，(2)知，原命题成立.

例 5 对于坐标平面上的格点 X，若线段 OX 上不含其他的格点，则称点 X 从原点 O

可见.求证:对任意正整数 n,存在面积为 n^2 的正方形 $ABCD$,使得在此正方形内部无从原点可见的格点.

证明 注意到格点 (x,y) 从原点可见当且仅当 x,y 互素,由此问题转化为求一个正方形 $ABCD$,使得其内部的每一格点 (x,y) 满足 x 与 y 不互素.设 $P_1,P_2,\cdots$ 是一列不同的质数,在 $n\times n$ 的矩阵 M 中,第一行的元素为前 n 个质数,第 2 行的元素为随后的 n 个质数,依此下去,设 m_i 为 M 中第 i 行元素的乘积,M_j 是 M 中第 j 列元素的乘积,则 $m_1,m_2,\cdots,m_n$ 两两互素,$M_1,M_2,\cdots,M_n$ 两两互素.下面,考虑同余式

$$\begin{cases}x\equiv-1(\bmod m_1),\\x\equiv-2(\bmod m_2),\\\vdots\\x\equiv-n(\bmod m_n).\end{cases}$$

由孙子定理,在 $\bmod m_1m_2\cdots m_n$ 下有唯一解 $a(a\in\mathbf{N}_+)$.

类似地,同余式

$$\begin{cases}y\equiv-1(\bmod M_1)\\y\equiv-2(\bmod M_2)\\\vdots\\y\equiv-n(\bmod M_n)\end{cases}$$ 在 $\bmod M_1M_2\cdots M_n$ 下有唯一解 $b(b\in\mathbf{N}_+)$.

在以 (a,b) 和 $(a+n,b+n)$ 为相对顶点的正方形中,其内部的格点满足 $(a+r,b+s)$,其中 $0<r<n,0<s<n$.

下面证明这样的点从原点不可见.事实上,因为 $a\equiv-r(\bmod m_r),b\equiv-s(\bmod M_s)$,所以,矩阵 M 的第 r 行 s 列的质数可以整除 $a+r$、$b+s$,故格点 $(a+r,b+s)$ 从原点不可见.

例 6 若 a、b 是互素的正整数,求证:

$$\left[\frac{a}{b}\right]+\left[\frac{2a}{b}\right]+\cdots+\left[\frac{b-1}{b}a\right]=\frac{1}{2}(a-1)(b-1).$$

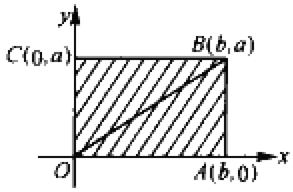


图 7-6

证明 如图 7-6 所示,矩形 $OABC$ 的四顶点为 $O(0,0)$,$A(b,0)$,$B(b,a)$ 和 $C(0,a)$,在此矩形内部的所有整点 (x,y) 满足 $1\leqslant x\leqslant b-1,1\leqslant y\leqslant a-1$,这些整点共有 $(a-1)\cdot(b-1)$ 个.

而矩形的对角线 OB 的方程为 $y=\frac{a}{b}x$,因为 $(a,b)=1$,而当 $x=1,2,\cdots,b-1$ 时,$y=\frac{a}{b}x$ 不可能是整数,也即 OB 上没有整点,这样位于 OB 下方的三角形与位于 OB 上方的三角形内部的格点个数相等,都等于 $\frac{1}{2}(b-1)(a-1)$.

另一方面，$\sum_{k=1}^{b-1}\left[\frac{ka}{b}\right]$就表示$\triangle OAB$的内部的格点个数.

因此$\sum_{k=1}^{b-1}\left[\frac{ka}{b}\right]=\frac{1}{2}(a-1)(b-1)$.

评注 事实上，此题与本节开头给出的定理2相似，证法也大同小异，都是用两种不同方法数某一个图形F内的格点个数，根据两种计算方法得到的两个式子恒等，于是便达到了证明的效果.

例7 求平面直角坐标系中格点凸五边形的周长的最小值.

分析 对于复平面上两点Z_1和Z_2(就用顶点的符号表示对应的复数)的距离为$|Z_1-Z_2|$，由于Z_1和Z_2都是格点，故$|Z_1-Z_2|$的值只能是$1,\sqrt{2},2,\sqrt{5},\cdots$，然后对整点凸五边形的各边长的取值进行分类，并对其周长作比较即得.

解 设此凸五边形的五个顶点依次为A_1,A_2,A_3,A_4和A_5. 坐标为$A_j(x_j,y_j)$，并用复数表示顶点：$A_j=x_j+iy_j$，$j=1,2,3,4,5$. 这里i为虚数单位.

记$Z_j=A_{j+1}-A_j$，$j=1,2,3,4,5$. 记$A_6=A_1$，则有(1)Z_j的实部与虚部都是整数，且$|Z_j|\neq0$(从而$|Z_j|\geqslant1$)；

(2)$Z_1+Z_2+Z_3+Z_4+Z_5=0$；

(3)凸五边形$A_1A_2\cdots A_5$的周长为$|Z_1|+|Z_2|+\cdots+|Z_5|$.

由凸性知，任意两个Z_j，$Z_k(j\neq k)$不具有同一方向，又由(1)知，若某个Z_j，有$|Z_j|\neq1$，则Z_j只能是$\sqrt{2},2,\sqrt{5},\cdots$.

$Z_1,Z_2,\cdots,Z_5$中模为1的个数至多有4个：$\pm1,\pm i$.

如果$|Z_1|,|Z_2|,\cdots,|Z_5|$中1的个数恰为4，由(2)知，余下一个为0，与(1)相违.

如果$|Z_1|,|Z_2|,\cdots,|Z_5|$中1的个数恰为3，(若剩下两个的模都为$\sqrt{2}$，注意模为$\sqrt{2}$的至多只有4个：$1\pm i,-1\pm i$，则它们不会满足(2))，于是，此时周长$\geqslant1+1+1+\sqrt{2}+2=5+\sqrt{2}$.

如果$|Z_1|,|Z_2|,\cdots,|Z_5|$中恰有两个1，剩下的3个都为$\sqrt{2}$，此时周长为$1+1+\sqrt{2}+\sqrt{2}+\sqrt{2}=2+3\sqrt{2}$.

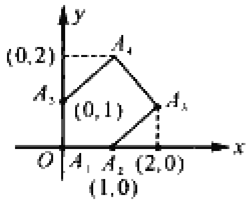


图7-7

其他情况，周长不小于$1+4\sqrt{2}$.

而$2+3\sqrt{2}$是可以取到的：

取$A_1(0,0)$，$A_2(1,0)$，$A_3(2,1)$，$A_4(1,2)$，$A_5(0,1)$(如图7-7)，则凸五边形$A_1A_2A_3A_4A_5$的周长为$2+3\sqrt{2}$.

综上，格点凸五边形周长的最小值为$2+3\sqrt{2}$.

能力训练

1. 三角形三边均为整数，最大边长为 11 的三角形有(　　)个.

A. 32　　B. 34　　C. 36　　D. 40

2. 第一象限的整点(x,y)满足$x+y>8$，且$x\leqslant y\leqslant 8$，这样的整点(x,y)有(　　)个.

A. 16　　B. 18　　C. 20　　D. 24

3. 在直角坐标系中，以(199,0)为圆心，以 199 为半径的圆周上，整点的个数有(　　)个.

A. 2　　B. 4　　C. 8　　D. 16

4. 由直线$y=2x$和直线$x=100$及x轴所围的三角形OAB(O为原点)内整点的个数为______.

5. 在 1～1000 中使$\dfrac{x^2+y^2}{7}$为整数的数对(x,y)有______对.

6. 设平面区域$T=\{(x,y)\mid x>0,y>0,xy\leqslant 48\}$，则$T$内的格点有______个.

7. 已知三角形的三边之长都是小于 100 的整数，且成等差数列，问这样的三角形有多少个.

8. 求证：平面上存在不全在一直线上的 2008 个格点，任意两点之间的距离都是整数.

9. 对于给定的正整数a，求证：方程$x+\dfrac{1}{2}(x+y-1)(x+y-2)=a$，有且只有一个正整数解.

10. 设M为平面上坐标为$(p\times 1994,7p\times 1994)$的点，其中$p$为素数，求满足下述条件的直角三角形的个数：

(1)三角形的三个顶点都是整点，而且M是直角顶点；

(2)三角形的内心是坐标原点.

§7.3 格点的染色、覆盖及其他

知识扫描

闵可夫斯基定理　设 K 为 xOy 平面上的凸图形，关于原点对称，面积大于 4，证明：图形 K 必然覆盖一个不是坐标原点的格点.

证明　用与坐标轴平行的直线把平面分成一些 2×2 的正方形，再将盖住 K 的点的所有正方形平移到同一正方形中，因 K 的面积大于 4，这正方形中必有一点被含 K 的点的正方形盖住两次，即 K 中两个点 $A\neq B$，它们的横、纵坐标值之差都是 2 的倍数，因图形 K 关于原点对称，A 关于原点的对称点为 A'，则 $A'\in K$，设 $B(x_1,y_1)$，$A(x_2,y_2)$，则 $x_1-x_2=2m$，$y_1-y_2=2n$，$m,n\in\mathbf{Z}$，因此 A' 为 $(-x_2,-y_2)$，所以 $A'B'$ 中点的坐标为 $\left(\frac{x_1-x_2}{2},\frac{y_1-y_2}{2}\right)=(m,n)\neq(0,0)$. 由于 K 是凸图形，故 (m,n) 在 K 内.

格点的覆盖常常与格点多边形的面积问题联系在一起，它往往会涉及“构造”，“极端”的内容，正是由于这使格点的覆盖问题兼具“数学性”与“趣味性”.

格点的染色是利用“色彩”极为直观地将格点进行的一种分类（区分）. 在“染色”的前提下，格点与格点之间的“作用”更加明晰.

例题分析

例 1　求内部只含一个格点的圆的最大面积.

证明　如图 7-8，以任一格点为圆心，1 为半径所作的圆内部只有一个整点，其圆面积为 π，设 $\odot P$ 的面积大于 π，则 $\odot P$ 的半径大于 1，圆心应落在某个边长为 1 的格点正方形内部或边上，记此正方形为 $ABCD$，若 $\odot P$ 的内部只含 1 个格点，则 A,B,C,D 中至多有一点在此圆的内部，因而至少有一对顶点不在 $\odot P$ 的内部，不妨设为 A，C. 由于 $\odot P$ 半径大于 1，A、C 不在 $\odot P$ 内部，故圆心 P 在以 A 为圆心，半径为 1 的 $\odot A$ 外，也在以 C 为圆心，半径为 1 的 $\odot C$ 外，但是 $\odot A$ 与 $\odot C$ 已覆盖了正方形 $ABCD$.

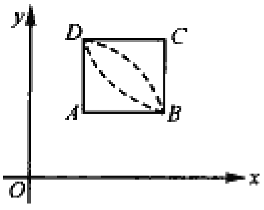


图 7-8

故 O 不在 $ABCD$ 内部和边界上，这与假设矛盾.

综上所述，内部只有一个格点的圆的最大面积为 π.

例 2 将数轴上每一个坐标为整数的点或染为红色，或染为蓝色，证明至少有一种颜色具有下述性质：即对每个正整数 k，都能找到无穷多个染了这种颜色的点，它们的坐标都能被 k 整除.

证明 分别以 A 和 B 表示红点和蓝点的集合.

假设结论不成立，即 A 中仅有有限个点其坐标为 a 的倍数，且 B 中仅有有限个点其坐标是 b 的倍数($a,b\in \mathbf{N}_+$)，这样在整个自然数集合中，就仅有有限个数是 ab 的倍数，但这是不可能的.

例 3 设 L 是直角坐标平面的一个子集，定义如下：

$L=\{(41x+2y,59x+15y)\mid x,y\in \mathbf{Z}\}$.

证明一切以坐标原点为中心的面积等于 2008 的平行四边形至少包含 L 中的两个点.

证明 取 $(x,y)=(0,0),(0,1),(1,0),(1,1)$，得到 L 中的四个点 $(0,0),(2,15),(41,59),(43,73)$.

设这四个整点为顶点构成基本区域 F，F 为平行四边形，其中没有其他整点.

这时，易知 F 的面积为 497.

将 F 平移形成平面的网络，其格点均为 L 中的点.

设平行四边形 P 以原点为对称中心，面积为 2008.

以原点为位似中心，作位似比为 $2:1$ 的位似变换，将 P 变成“$\frac{1}{2}P$”，这时面积为

$\frac{1}{4}\cdot 2008=502>497$.

所以将 $\frac{1}{2}P$ 的各块经过平行移动到 F 中后，必有两个点重合.

设这两个点为 $D_1(x_1,y_1)$，$D_2(x_2,y_2)$，分别沿 $\overrightarrow{OA_1}$，$\overrightarrow{OA_2}$ 平移，其中 $A_1(a_1,b_1)$，$A_2(a_2,b_2)$ 都是 L 中的点，则 $(x_1,y_1)+(a_1,b_1)=(x_2,y_2)+(a_2,b_2)$.

从而 $(a_1-a_2,b_1-b_2)=(a_1,b_1)-(a_2,b_2)=(x_2,y_2)-(x_1,y_1)$.

易知点 $D(x_2-x_1,y_2-y_1)\in P$(这是因为 $(x_1,y_1)\in\frac{P}{2}$，$(x_2,y_2)\in\frac{P}{2}$，而 $\frac{P}{2}$ 是以原点为中心的对称图形，所以 $(-x_1,-y_1)\in\frac{P}{2}$，则由 $\frac{P}{2}$ 的凸性，$\left(\frac{x_2-x_1}{2},\frac{y_2-y_1}{2}\right)\in\frac{P}{2}$，所以 $D(x_2-x_1,y_2-y_1)\in P$).

而点 $D(a_1-a_2,b_1-b_2)\in L$，并且 D 不同于 $(0,0)$.

所以 P 中至少有 L 中的两个点.

评注 本题的证明过程与闵可夫斯基定理的证明类似.

例 4 已知 m,n 是大于 7 的整数,考虑 $m\times n$ 个点构成的矩形点阵,将其中的 k 个点染为红色,使得任意具有两条直角边平行于矩形的边的直角三角形的三个顶点是不同为红色的点,求 k 的最大值.

解 假设有 m 行 $n(n\leqslant m)$ 列,则最大值至少是 $m+n-2$,因为任取一行、一列,则除这一行、一列的公共点之外,将这一行、一列的其他所有点均涂为红色,即为满足条件的情形.

下面用数学归纳法证明在 $m\times n$ 点阵中,红点数$\leqslant m+n-2$ 个.

当 $n=2$ 时,若红点数为 $m+n-1=m+1$,则必存在一行有 2 个红点,则此两列无其他红点,矛盾!

当 $n=3$ 时,若红点数为 $m+n-1=m+2$,则必存在一行有 2 个红点,则此两列无其他红点,另一列最多有 $m-1$ 个红点,矛盾.

若 $n\leqslant k$ 时,在 $m\times n$ 的点阵中,红点数$\leqslant m+n-2$ 个,假设 $n=k+1$ 时,在 $m\times n$ 点阵中有 $m+n-1=m+k$ 个红点,由抽屉原则,必有一行有 2 个红点,此 2 个红点所在的列中无其他红点,将此两列从点阵中去掉,变为 $m\times(k-1)$ 点阵中有 $m-k-2$ 个红点的情况,由归纳假设,此种情况不会发生.

故在 $m\times n$ 点阵中,红点数$\leqslant m+n-2$.

综上所述,k 的最大值为 $m+n-2$.

例 5 设 n 为任意给定的正整数,T 为平面上所有满足 $x+y<n$,x、y 为非负整数的点(x,y)所组成的集合,T 中每一点(x,y)均被染上红色或蓝色,满足:若(x,y)是红色,则 T 中所有满足 $x'\leqslant x,y'\leqslant y$ 的点(x',y')均为红色,如果 n 个蓝点的横坐标各不相同,则称这 n 个蓝点所组成的集合为一个 X-集;如果 n 个蓝点的纵坐标各不相同,则称这 n 个蓝点所组成的集合为一个 Y-集,求证:

X-集的个数和 Y-集的个数一样多.

证明 设红点个数为 m,X-集合数目为 t,Y-集合数目为 s,对 $m\left(0\leqslant m\leqslant\frac{n(n+1)}{2}\right)$进行归纳证明.

(1)当 $m=0$ 时,由乘法计数原理,$s=t=n!$,命题成立.

(2)假设 $m=k\left(0\leqslant k<\frac{n(n+1)}{2}\right)$时命题成立.

而对于 $m=k+1$,设点 $P(x_0,y_0)$是使 x_0+y_0 最大的红点之一,那么,将 P 改为蓝点,由于不存在其他红点(x,y),$x\geqslant x_0$,$y\geqslant y_0$,因此,这仍然是一个满足条件的集合,记为 T',对它类似地定义 t',s'.

对于 T',设它在 $x=i(0\leqslant i\leqslant n-1)$列上的蓝点有 a_i 个,在 $y=j(0\leqslant j\leqslant n-1)$行上的

蓝点有 b_j 个，那么，$t'=\prod_{i=0}^{n-1}a_i$，$s'=\prod_{j=0}^{n-1}b_j$.

由归纳法假设有 $t'=s'$，即 $\prod_{i=0}^{n-1}a_i=\prod_{j=0}^{n-1}b_j$.

对于改变前的集合 T，有 $t=(\prod_{\substack{i=0\\i\neq x_0}}^{n-1}a_i)(a_{x_0}-1)$，$s=(\prod_{\substack{j=0\\j\neq y_0}}^{n-1}b_j)(b_{y_0}-1)$.

在 $x=x_0$ 列上，纵坐标大于等于 y_0 的 T 中的点有 $n-x_0-y_0$ 个，所以 $a_{x_0}=n-x_0-y_0$，同理，$b_{y_0}=n-x_0-y_0$，故 $a_{x_0}=b_{y_0}$.

于是 $(\prod_{\substack{i=0\\i\neq x_0}}^{n-1}a_i)(a_{x_0}-1)=(\prod_{\substack{j=0\\j\neq y_0}}^{n-1}b_j)(b_{y_0}-1)$，即 $t=s$，故对 $m=k+1$ 时，命题也成立.

因此，对一切 $0\leqslant m\leqslant\frac{n(n+1)}{2}$ 命题都成立.

能力训练

1. 内部至少有两个格点的格点多边形的面积的最小值是多少？

2. 求证格点凸五边形的内部必有一个格点.

3. 在直角坐标系中作闭折线，使折线的每个结点都是格点，而折线的各段之长都相等，证明：这样的折线的段数必有偶数.

4. 在直角坐标平面上给定格点凸五边形 $ABCDE$，证明：以其对角线在形内的交点为顶点的凸五边形 $A_1B_1C_1D_1E_1$ 的内部或周界上至少有一个整点.

5. 证明：平面内格点 (x,y)，$x,y\in\mathbf{Z}$，可以用红蓝两种颜色染色，使得任一条平行于 y 轴的直线上仅有有限多个红点，任一条平行于 x 轴的直线上仅有有限多个蓝点.

参考答案

第一章　整除

§1.1　整除与余数

1. 证明：由于 $(ad+bc)-(ab+cd)=a(d-b)+c(b-d)=(a-c)(d-b)$，

所以 $(a-c)\mid((ad+bc)-(ab+cd))$.

又因为 $(a-c)\mid(ab+cd)$，

所以 $(a-c)\mid(ad+bc)$.

2. 证明：据题意 a^2+ab+1 被 b^2+ab+1 整除，则 $(a^2+ab+1,b^2+ab+1)=b^2+ab+1$，

又由于 $b(a^2+ab+1)-a(b^2+ab+1)=b-a$，若 $a\neq b$，

由裴蜀定理可知 $(b^2+ab+1)\mid(b-a)$，

即 $b^2+ab+1\leqslant b-a\leqslant b$，

矛盾！

则 $a\neq b$ 不成立，即 $a=b$.

3. 解：共有 7 组.

由于是考虑被 11 整除的问题，所以可以将原数列改写为 1，4，−3，−1，5，−3，−1，3，−3，−1.

设其前 n 项之和为 S_n，

则 $S_1=S_4=S_{10}=1$，$S_2=S_8=5$，$S_3=S_7=S_9=2$.

这样共有 $C_3^2+C_2^2+C_3^2=7$ 组数能被 11 整除，它们是 S_4-S_1，$S_{10}-S_1$，$S_{10}-S_4$，S_8-S_2，S_7-S_3，S_9-S_3，S_9-S_7，所以相邻若干个数之和能被 11 整除的数组共有 7 组.

4. 用归纳法证明：当 $n=1$ 时，$5\mid5$.

设 $n=m$ 时，$5^m \mid \overline{a_1a_2\cdots a_m}$，其中 $a_i(i=1,2,\cdots,m)$ 为一位奇数.

当 $n=m+1$ 时，考查 $\overline{1a_1a_2\cdots a_m}$，$\overline{3a_1a_2\cdots a_m}$，$\cdots$，$\overline{9a_1a_2\cdots a_m}$.

因为它们的差 2×10^m，4×10^m，6×10^m，8×10^m 不能被 5^{m+1} 整除.

所以这 5 个数被 5^{m+1} 整除的余数两两不等.

所以，这五个数中存在一个能被 5^{m+1} 整除的数.

5. 证明：先将 20790 分解得 $20790=2\times3\times5\times7\times9\times11$，由 6 个整数乘积组成.

又可想到：在任给 $i+1$ 个数中必有 2 个数的差为 i 的倍数.

设 12 个正整数为 $a_i(i=1,2,\cdots,12)$.

易知，这 12 个数中必有 2 个数（不妨设为 a_1，a_2，且 $a_2>a_1$）之差为 11 的倍数，即 $a_2-a_1=11k_1$，k_1 为整数.

在剩下的 10 个数中必有 2 个数（不妨设为 a_3，a_4，且 $a_3<a_4$）之差是 9 的倍数，即 $a_4-a_3=9k_2$，k_2 为整数.

依此类推得：$a_6-a_5=7k_3$，$a_8-a_7=5k_4$，$a_{10}-a_9=3k_5$，k_3，k_4，k_5 均为整数.

对剩下的 2 个数（即 a_{11}，a_{12}，设 $a_{11}<a_{12}$）若至少有 1 个为偶数，则

$a_{11}a_{12}(a_2-a_1)(a_4-a_3)(a_6-a_5)\cdots(a_{10}-a_9)=2k\cdot11k_1\cdot9k_2\cdot7k_3\cdot5k_4\cdot3k_5=20790\cdot M$（$M$ 为整数），

若剩下的 2 个数均为奇数，则 $a_{12}-a_{11}=2k$（k 为整数），

于是，$(a_{12}-a_{11})(a_2-a_1)(a_4-a_3)\cdots(a_{10}-a_9)=20790\cdot N$，其中 N 为整数.

6. 解：a 的值为 1.

根据题设 $(a+d)^2=(a-d)^2+4ad>(b-c)^2+4bc=(b+c)^2$，

从而 $a+d>b+c$，即 $k>m$.

又因为 $a(2^k-a)=b(2^m-b)$，

即 $(b+a)(b-a)=2^m(b-2^{k-m}a)$，

于是 $2^m\mid(b+a)(b-a)$，

因为 a，b 均为奇数，所以有 $b+a$，$b-a$ 均为偶数，但两者之差 $2a$ 不是 4 的倍数，从而 $b+a$，$b-a$ 中恰有一个数不能被 4 整除.

所以 $2^{m-1}\mid(b+a)$ 或 $2^{m-1}\mid(b-a)$，

注意到 $0<b-a<b<\frac{1}{2}(b+c)=2^{m-1}$，

及 $b+a<b+c=2^m$，

从而 $2^{m-1}\mid(b+a)$ 且 $b+a=2^{m-1}$，

于是 $b-a=2(b-2^{k-m}a)$，

进而有 $a=2^{2m-k-2}$，因为 a 是奇数，

所以必有 $a=1$.

7. 证明：由带余除法，得 $n=mq+r, 0\leqslant r<m$，而 $q\geqslant 0$，

如果 q 是偶数，由 $a^n+1=(a^{mq}-1)a^r+(a^r+1)$，

必有 $(a^m+1)\mid(a^r+1)$，

但 $0<a^r+1<a^m+1$，这不可能成立.

因此 q 是奇数.

由 $a^n+1=(a^{mq}+1)a^r-(a^r-1)$，并注意 $(a^m+1)\mid(a^{mq}+1)$，

我们推出 $(a^m+1)\mid(a^r-1)$，但 $0\leqslant r<m$，

必须 $a^r-1=0$，即 $r=0$，

所以，$n=mq$.

即 $m\mid n$.

8. 证明：由题意，$a_0=2, a_1=1, a_2=3, a_3=4, a_4=7, a_5=11$.

由 $a_1\cdot a_3=4=a_2^2-5, a_3\cdot a_5=44=a_4^2-5$.

猜想：$a_{2k-1}\cdot a_{2k+1}=a_{2k}^2-5$.

$k=1$ 时，显然成立.

假设 $k=t$ 时，命题成立，即 $a_{2t-1}\cdot a_{2t+1}=a_{2t}^2-5$.

对于 $k=t+1$，只需证明 $a_{2t+1}\cdot a_{2t+3}=a_{2t+2}^2-5$

$\Leftrightarrow (a_{2t-1}+a_{2t})(a_{2t}+2a_{2t+1})=(2a_{2t}+a_{2t-1})^2-5$

$\Leftrightarrow 2a_{2t+1}a_{2t-1}+(2a_{2t+1}+a_{2t-1})a_{2t}+a_{2t}^2=4a_{2t}^2+4a_{2t-1}a_{2t}+a_{2t-1}^2-5$

$\Leftrightarrow 2a_{2t+1}a_{2t-1}+(3a_{2t-1}+2a_{2t})a_{2t}+a_{2t}^2=4a_{2t}^2+4a_{2t-1}a_{2t}+a_{2t-1}^2-5$

$\Leftrightarrow 2a_{2t+1}a_{2t-1}=a_{2t}^2+a_{2t-1}a_{2t}+a_{2t-1}^2-5$

$\Leftrightarrow 2a_{2t+1}a_{2t-1}=a_{2t}^2+a_{2t+1}a_{2t-1}-5$

$\Leftrightarrow a_{2t+1}a_{2t-1}=a_{2t}^2-5$，即归纳假设.

所以结论对 $k=t+1$ 也成立.

所以 $a_{2k-1}\cdot a_{2k+1}=a_{2k}^2-5$ 对 $k\in\mathbf{N}_+$ 成立.

故 $(a_{2k-1}+1)(a_{2k+1}-1)=a_{2k-1}\cdot a_{2k+1}+a_{2k+1}-a_{2k-1}-1=a_{2k}^2+a_{2k}-6$

$$=(a_{2k}+3)(a_{2k}-2).$$

所以 $p\mid(a_{2k-1}+1)(a_{2k+1}-1)$.

又 $p\mid(a_{2k}-2)=(a_{2k+1}-1)-(a_{2k-1}+1)$，

故有 $p\mid(a_{2k-1}+1), p\mid(a_{2k+1}-1)$，

所以 p 也是 $a_{2k+1}-1$ 的质因子.

9. 解：$n=4k(k\in\mathbf{N}_+)$ 为 n 的值.

根据题设，$(x_1y_1+x_2y_2+\cdots+x_ny_n)+(x_1z_1+x_2z_2+\cdots+x_nz_n)+(y_1z_1+y_2z_2+\cdots+y_nz_n)=0$.

故这 $3n$ 个积中，$+1$ 和 -1 的个数相同.

即 $2|3n$.

又因为 $\prod_{i=1}^{n}x_iy_i\cdot\prod_{i=1}^{n}x_iz_i\cdot\prod_{i=1}^{n}y_iz_i=\prod_{i=1}^{n}x_i^2\cdot\prod_{i=1}^{n}y_i^2\cdot\prod_{i=1}^{n}z_i^2=1$.

故 $3n$ 个积中，-1 有偶数个.

从而 $4|3n$，即 $n=4k(k\in\mathbf{N}_+)$ 这是充分的，令 $y_1=y_2=\cdots=y_{2k}=z_{k+1}=z_{k+2}=\cdots=z_{3k}=-1$，其余的数为 1，即可满足题意.

所以 $n=4k(k\in\mathbf{N}_+)$.

10. 证明：设前 $2n$ 个自然数写成随意一行为 $a_1,a_2,a_3,\cdots,a_{2n-1},a_{2n}$，其中 $1\leqslant a_i\leqslant 2n$，$a_i\neq a_j(i\neq j)$，$(i,j=1,2,3,\cdots,2n)$，那么，对应的和数为 $1+a_1,2+a_2,\cdots,2n-1+a_{2n-1}$，$2n+a_{2n}$.

这些和数各自被 $2n$ 除，所得余数只能为下列 $2n$ 个情形之一：$0,1,2,\cdots,2n-2,2n-1$.

若能证得 $2n$ 个余数不可能全部出现，则问题得以解决. 从正面解决比较困难，于是从反面考虑.

假如这 $2n$ 个余数都出现，则其和为 $r_{2n}=0+1+2+\cdots+(2n-1)=2n^2-n>0$.

此和应当与题设的 $2n$ 个和数的总和除以 $2n$ 后所得到的余数关于模 $2n$ 同余（即除以 $2n$ 余数相同），这表明余数为零. 矛盾.

11. 证明：由于 $(a,b)=1$，故有整数 x,y 使 $ax+by=1$.

由带余除法，$x=bq+r,0\leqslant r<b$，

令 $aq+y=-s$，则得出 $ar-bs=1$，因 $b\neq1$，故

$r\neq0$，即 $0<r<b$，由此即知 $0<s<a$.

12. 解：设这些连续正整数共有 n 个（$n>1$）. 最小者为 a，则 $a+(a+1)+\cdots+(a+n-1)=6^3$.

即 $n(2a+n-1)=432$.

显然 $n\not\equiv 2a+n-1 \pmod 2$，即 n、$2a+n-1$ 的奇偶性不相同.

因为 $a\geqslant1$，故 $2a+n-1>n$.

由于 $432=2^4\cdot3^3$，$n<\sqrt{432}<21$，

所以 n 可取的值为 2,3,4,6,8,9,12,16,18.

仅在 n 取 3,9,16 时，$\frac{432}{n}$ 与 n 的奇偶性不同.

故解只有三种：$(n,a)=(3,71),(9,20),(16,6)$.

13. 证明：证明这连续的 18 个数中一定有两个数是 9 的倍数，且它们的各位数字之和能被 9 整除.

由于小于或等于 2005 的正整数的各位数字之和最大是 28，所以，这两个数的各位数字之和只可能是 9，18 或 27.

若这两个数中有一个其各位数字之和为 27，则只可能是 999 或 1998 或 1989 或 1899，前两数均可以被 27 整除；若为 1989，则 1980 或 1998 满足条件；若为 1899，则 1890 或 1908 满足条件.

若这两个数各位数字之和均为 18，则这两个数一定有一个是偶数，这个数能被 18 整除.

14. 首先证明：如果 x、y 是正整数，n 是非负整数，且满足 $\frac{xy}{x+y}>n$，则

$$\frac{xy}{x+y}\geqslant n+\frac{1}{n^2+2n+2}.$$

实际上，$\frac{xy}{x+y}>n$ 可以改写成 $(x-n)(y-n)>n^2$.

于是，有 $x>n$，$y>n$.

设 $x=n+d_1$，$y=n+d_2$，则 $d_1d_2=(x-n)(y-n)=n^2+r$.

这里 d_1，d_2，r 均是正整数.

因为 $(d_1-1)(d_2-1)\geqslant 0$，

所以 $(d_1+d_2)\leqslant 1+d_1d_2=1+n^2+r$.

又因为对于任意的 $A>0$，$r\geqslant 1$，有不等式 $\frac{r}{A+r}\geqslant\frac{1}{A+1}$.

则

$$\begin{aligned}\frac{xy}{x+y}&=\frac{n^2+d_1d_2+n(d_1+d_2)}{2n+d_1+d_2}\\&=n+\frac{r}{2n+d_1+d_2}\\&\geqslant n+\frac{r}{2n+n^2+1+r}\\&\geqslant n+\frac{1}{n^2+2n+2}.\end{aligned}$$

当且仅当 $x=n+1$，$y=n^2+n+1$ 或 $y=n+1$，$x=n^2+n+1$ 时，上式等号成立.

根据已知条件，存在正整数 p、q，使得 $c(c^2-c+1)=pab$，$a+b=q(c^2+1)$.

则 $\frac{c(c^2-c+1)}{c^2+1}=\frac{pqab}{a+b}=\frac{xy}{x+y}$，

其中 $x=pqa$，$y=pqb$，且 $\frac{xy}{x+y}=c-1+\frac{1}{c^2+1}>c-1$.

因此，由前面证明的结论可得

$\frac{xy}{x+y} \geqslant c-1+\frac{1}{(c-1)^2+2(c-1)+2}=\frac{c(c^2-c+1)}{c^2+1}$.

等号成立条件是 $x=c, y=(c-1)^2+(c-1)+1=c^2-c+1$ 或 $x=c^2-c+1, y=c$.

由于 c 与 c^2-c+1 互质，由 $x=pqa, y=pqb$，可知 $p=q=1$.

故 $a=c, b=c^2-c+1$ 或 $a=c^2-c+1, b=c$.

15. 解：因为 $792=8\times9\times11$，

所以，数字 $\overline{13xy45z}$ 能被 8、9、11 整除.

由 $8|\overline{13xy45z}$，知 $8|\overline{45z}$，

而 $\overline{45z}=450+z=448+(z+2)$，因此 $8|(z+2)$，故 $z=6$.

由 $9|\overline{13xy45z}$，

知 $9|(1+3+x+y+4+5+z)$，

而 $1+3+x+y+4+5+z=x+y+19=18+(x+y+1)$，

因此，$9|(x+y+1)$，

故 $x+y=8$ 或 17.

由 $11|\overline{13xy45z}$，

知 $11|(6-5+4-y+x-3+1)$，

而 $6-5+4-y+x-3+1=x-y+3$，

因此 $x-y=-3$ 或 $x-y=8$.

此时，有两种可能：

(1)若 $x+y$ 为偶数，则 $x+y=8$ 且 $x-y=8$，从而 $x=8, y=0$；

(2)若 $x+y$ 为奇数，则 $x+y=17$ 且 $x-y=-3$，从而 $x=7, y=10$ 这不可能.

所以，唯一的正整数解为 1380456.

§1.2 最大公因数和最小公倍数

1. 证明：由于 $\frac{a+1}{b}+\frac{b+1}{a}=\frac{a^2+b^2+a+b}{ab}$ ①

设 $(a,b)=d$，则 $d^2|ab$.

显然 $d^2|(a^2+b^2)$，

由①式，$d^2|(a+b)$，

于是 $a+b\geqslant d^2$，$\sqrt{a+b}>d$，

即 $(a,b)\leqslant\sqrt{a+b}$.

所以 a 和 b 的最大公约数不超过 $\sqrt{a+b}$.

2. 证明：由于 $(a,b)=1$，故 $ax+by=n$ 必有一组整数解 (x,y).

我们不妨设 $0\leqslant x<b$，这样，当 $n>ab-a-b$ 时，

我们有 $by=n-ax>ab-a-b-ax$

$\geqslant ab-a-b-a(b-1)$

$=-b$.

故 $y>-1$ 也是非负整数.

当 $n=ab-a-b$ 时,如果方程有非负整数解 (x,y),则 $ab=(x+1)a+(y+1)b$,

故 $a\mid(y+1)b$,

因为 $(a,b)=1$,所以 $a\mid(y+1)$,

因为 $y+1>0$,故 $y+1\geqslant a$,

同理 $x+1\geqslant b$,

于是 $ab=(x+1)a+(y+1)b\geqslant ab+ab=2ab$.

矛盾,故原命题成立.

3. 证明:当 $1\leqslant k\leqslant 2^n-1$ 时,由正整数二进制表示的唯一性推知,2^n 个数 $a_0+2a_1+\cdots+2^{n-1}a_{n-1}$($a_i=0$ 或 1)恰给出了 $0,1,2,\cdots,2^n-1$,故 k 是 2^{n-1}(从而是 m 的)不同约数之和.

当 $2^n-1<k\leqslant m$ 时,由带余除法 $k=(2^n-1)t+r$,$0\leqslant r<2^n-1$.

显然 $t\leqslant 2^{n-1}$,故由上面的结论知,r 和 t 都是 2^{n-1} 的不同约数之和,于是 $(2^n-1)t$ 可表示为 $m=2^{n-1}(2^n-1)$ 的不同约数之和(这些约数与表示 r 的约数显然不会有相同者).

4. 解:设 $d_n=(100+n^2,100+(n+1)^2)$.

则有 $d_n\mid(100+n^2)$,$d_n\mid(100+(n+1)^2)$,

所以 $d_n\mid(100+(n+1)^2-100-n^2)$,

即 $d_n\mid(2n+1)$.

又因为 $2(100+n^2)=n(2n+1)+200-n$,

所以 $d_n\mid(200-n)$,$d_n\mid((2n+1)+2(200-n))$,

即 $d_n\mid 401$,

所以 $1\leqslant d_n\leqslant 401$.

又当 $n=200$ 时,有 $100+n^2=100+200^2=100\cdot 401$,

$100+(n+1)^2=100+201^2=101\cdot 401$,

所以 d_n 能达到 401.

即 $(d_n)_{\max}=401$.

5. 证明:设 $d\in\mathbf{N}$ 是 $C_n^k,C_{n+1}^k,\cdots,C_{n+k}^k$ 的公约数,则 d 也是 $C_n^{k-1}=C_{n+1}^k-C_n^k$,$C_{n+1}^{k-1}=C_{n+2}^k-C_{n+1}^k$,$\cdots$,$C_{n+k-1}^{k-1}=C_{n+k}^k-C_{n+k-1}^k$ 的公约数.

同理,d 也是 $C_n^{k-2},C_{n+1}^{k-2},\cdots,C_{n+k-2}^{k-2},C_n^{k-3},C_{n+1}^{k-3},\cdots,C_{n+k-3}^{k-3},\cdots$ 的公约数.

如此继续，d 是 C_n^0 的约数，

因此，$C_n^k, C_{n+1}^k, \cdots, C_{n+k}^k$ 的最大公约数等于 1.

6. 证明：据题意，对任给的正整数 k，有

$Q(n)=[n, n+1, n+2, \cdots, n+k]$

$Q(n+1)=[n+1, n+2, n+3, \cdots, n+k, n+k+1]$

设 $t=[n+1, n+2, \cdots, n+k]$，

则 $Q(n)=[n, t]$，$Q(n+1)=[t, n+k+1]$，

此时，取 $n=p(k+1)$，p 是大于 $k+1$ 的质数.

因 $Q(n)=[p(k+1), t]$，$Q(n+1)=[t, (p+1)(k+1)]$，

即 $Q(n)=[p, m]$，$Q(n+1)=[m, p+1]$，$m=[k+1, t]$，

显然，由于 $p>k+1$ 且 p 是质数，则 p 与 $n+1, n+2, \cdots, n+k$ 都互质，而 $p+1$ 为偶数.

所以有 $Q(n)=pm$，$Q(n+1)\leqslant\frac{m(p+1)}{2}$，

而 $pm-\frac{m(p+1)}{2}=\frac{m(p-1)}{2}>0$，

即 $Q(n+1)\leqslant\frac{m(p+1)}{2}<pm=Q(n)$，

故原命题 $Q(n+1)<Q(n)$ 成立.

7. 解：设 100 个正整数 $a_1, a_2, \cdots, a_{100}$ 的最大公约数为 d，并令 $a_j=da'_j (1\leqslant j\leqslant 100)$.

由于 $a_1+a_2+\cdots+a_{100}=d(a'_1+a'_2+\cdots+a'_{100})$

$=101101$

$=101\times 1001$

于是 $a'_1, a'_2, \cdots, a'_{100}$ 不可能都是 1，从而 $a'_1+a'_2+\cdots+a'_{100}\geqslant 1\times 99+2=101$.

从而 $d\leqslant 1001$.

另一方面，取 $a_1=a_2=\cdots=a_{99}=1001$，$a_{100}=2002$，这时满足 $a_1+a_2+\cdots+a_{100}=101101$.

而 $(1001, 1001, \cdots, 1001, 2002)=1001$，

所以 $a_1, a_2, \cdots, a_{100}$ 的最大公约数的最大可能值为 1001.

8. 解：设 $(4n+5, 7n+6)=d>1$，则

$d\mid(4n+5)$，$d\mid(7n+6)$.

从而 $d\mid(7n+6-(4n+5))=3n+1$，

$d\mid((4n+5)-(3n+1))=n+4$，

$d\mid((3n+1)-2(n+4))=n-7$，

$d\mid((n+4)-(n-7))=11.$

因为 11 是素数，则 $d=11$.

设 $n-7=11k$，则

$0<n=11k+7<50$. 解得 $k=0,1,2,3$.

于是 $n=7,18,29,40$.

9. 解：如果三个数相等，则有$[a,b,c]=a$，与$[a,b,c]=a+b+c$ 矛盾.

不失一般性，假设 $a\leqslant b\leqslant c$，且等号不同时成立，则 $a+b<2c$.

因此，$c<a+b+c<3c$.

因为$[a,b,c]$是 c 的倍数，所以有$[a,b,c]=2c$.

于是，$a+b=c$，$[a,b,c]=2a+2b$，

又 $b\mid(2a+2b)$，所以 $b\mid 2a$.

从 $a\leqslant b$ 可以推知，$b=a$ 或 $b=2a$.

如果 $b=a$，则 $c=a+b=2a$，因此，$[a,b,c]=[a,a,2a]=2a$.

但是 $a+b+c=a+a+2a=4a$，矛盾.

如果 $b=2a$，则 $c=a+b=a+2a=3a$.

$[a,b,c]=[a,2a,3a]=6a=a+b+c$.

所以，满足题目要求的三元正整数形式为$(a,2a,3a)(a\geqslant 1)$.

10. 解：(1)因为$(a+b+c)\mid(a^2+b^2+c^2)$，$(a+b+c)\mid(a^3+b^3+c^3)$，

则$(a+b+c)\mid[(a+b+c)^2-a^2-b^2-c^2]$，

即$(a+b+c)\mid(2ab+2bc+2ca)$.

又$(a+b+c)(a^2+b^2+c^2-ab-bc-ca)=a^3+b^3+c^3-3abc$.

故$(a+b+c)\mid 3abc$.

设质数 p 满足 $p^{\alpha}\parallel(a+b+c)(\alpha\geqslant 1)$(记号 $\parallel$ 见本书第 18 页)，

若存在 $p\geqslant 5$，则 $p\mid abc$，不妨设 $p\mid a$.

因为 $p\mid 2(ab+bc+ca)$，所以 $p\mid bc$.

不妨设 $p\mid b$，因为 $p\mid(a+b+c)$，所以 $p\mid c$.

则 $p\mid(a,b,c)$，矛盾.

所以 $p=2$ 或 3.

故 $a+b+c=2^m\times 3^n(m、n\geqslant 0)$.

若 $n\geqslant 2$，则 $3\mid(a+b+c)$，$3\mid abc$，$3\mid(ab+bc+ca)$.

仿上即可推出 $3\mid(a,b,c)$，矛盾.

故 $n=0$ 或 1.

设 $a+b+c=2^m\cdot k(k=1$ 或 $3)$，则 $2^m\mid abc$，

因为$(a,b,c)=1$，不妨设a为奇数.

又$2^m|(a+b+c)$，不妨设b为奇数，c为偶数，所以$2^m|c$.

由$2^m|(2ab+2bc+2ca)$，则$2^{m-1}|ab$.

从而，$m=0$或1.

又$a+b+c\geqslant3$，所以，$a+b+c=3$或6.

分别验证得，$(a,b,c)=(1,1,1)$或$(1,1,4)$.

(2)易得$a^n+b^n+c^n=(a+b+c)(a^{n-1}+b^{n-1}+c^{n-1})-(ab+bc+ca)(a^{n-2}+b^{n-2}+c^{n-2})+abc(a^{n-3}+b^{n-3}+c^{n-3})$ ①

又$(a+b+c)|(a^{2004}+b^{2004}+c^{2004})$，$(a+b+c)|(a^{2005}+b^{2005}+c^{2005})$.

将$n=2007$代入式①得

$(a,b,c)|(a^{2007}+b^{2007}+c^{2007})$，与条件矛盾.

故不存在满足条件的(a,b,c).

§1.3 素数及算术基本定理

1. 证明：设d_1是n的一个正约数，则$d_2=\dfrac{n}{d_1}$也是n的一个正约数.

于是$\min\{d_1,d_2\}\leqslant\sqrt{n}$.

把n的所有正约数两两配对(当n为完全平方数时，$\sqrt{n}$除外)，从而正约数的总个数不超过$\sqrt{n}+\sqrt{n}=2\sqrt{n}$.

2. 解：由于10个连续正整数中必有数被$2^3,3^2,5,7$整除.

所以$n=2^{a_1}\cdot3^{a_2}\cdot5^{a_3}\cdot7^{a_4}\cdot11^{a_5}\cdots$其中，$a_1\geqslant3,a_2\geqslant2,a_3\geqslant1,a_4\geqslant1,\cdots$

由于n的正因数的个数为$(a_1+1)(a_2+1)\cdots=144$，

而$(a_1+1)(a_2+1)(a_3+1)(a_4+1)\geqslant4\cdot3\cdot2\cdot2=48$，

于是有$(a_5+1)(a_6+1)\cdots\leqslant3$.

所以至多有一个$a_j(j\geqslant5)$为正数，并且a_j只能为1或2.

考虑方程$(a_1+1)(a_2+1)(a_3+1)(a_4+1)(a_5+1)=144$.

关于$a_1\geqslant3,a_2\geqslant2,a_3\geqslant1,a_4\geqslant1,a_5=1$或2的所有的解，并使$n$最小，由此可得$a_1=5,a_2=2,a_3=a_4=a_5=1$.

即$n=2^5\cdot3^2\cdot5\cdot7\cdot11=110880$.

3. 解：设整数x使$q=x^3(p-x)$. ①

于是$x|q$.

因为q是素数，因此只能有$x=\pm1,x=\pm q$.

当$x=\pm q$时，由①有

$q^2|1$,这是不可能的(因为 q 是素数).

当 $x=-1$ 时,有 $p+q+1=0$,这也不可能.

当 $x=1$ 时,由①式得 $p=q+1$,

因为 p、q 都是素数,则 $p=3,q=2$.

4. 解:若 $2p+1$ 是自然数的方幂,即 $2p+1=m^n$,

则 m 为奇数.设 $m=2k+1$,则有

$2p+1=(2k+1)^n$,

从而 $2p=2k\cdot A$,其中 p 是素数,A 是大于 1 的整数.

即 $p=k\cdot A$,

由 p 是素数可知,$k=1$,因而 $m=3$.

即 $2p+1=3^n$, ①

由 $p\leqslant 1000$,则 $3^n\leqslant 2001$,

而不超过 2001 的 3 的幂仅有 $3,3^2,3^3,3^4,3^5,3^6$ 代入①式逐个计算可得,仅有 $2p+1=3^3$,使 p 为素数.

此时 $p=13$.

即符合题意的素数仅有 1 个,$p=13$.

5. 证明:设这 6 个数为 a_1,a_2,a_3,a_4,a_5,a_6.

若题设不成立,则可设

$(a_1,a_2,a_3,a_4,a_5)=d_1,(a_1,a_2,a_3,a_4,a_6)=d_2$,

$(a_1,a_2,a_3,a_5,a_6)=d_3,(a_1,a_2,a_4,a_5,a_6)=d_4$,

$(a_1,a_3,a_4,a_5,a_6)=d_5,(a_2,a_3,a_4,a_5,a_6)=d_6$,

其中,d_1,d_2,d_3,d_4,d_5,d_6 两两互质,且 $d_i\neq 1(i=1,2,\cdots,6)$.

不妨设 $d_1>d_2>d_3>d_4>d_5>d_6$,那么

$a_1=b_1d_1d_2d_3d_4d_5\geqslant b_1\times 3\times 5\times 7\times 11\times 13=15015\cdot b_1>10000$,矛盾!

因此,假设不真.

故 d_1,d_2,d_3,d_4,d_5,d_6 中必有一个为 1.

即从任意 6 个互质的四位数中能选出 5 个数是互质的.

6. 解:由条件(1),设 $n=75k(k\in\mathbf{N})$.

因为 $75=5^2\cdot 3$,所以 $n=5^2\cdot 3k$.

又设 $n=5^s\cdot 3^t p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$,其中 $p_i(i=1,2,\cdots,m)$ 为素数,α_i 为非负整数.

由条件(2),n 的素因数分解中,素数指数应满足 $(s+1)(t+1)(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_m+1)=75$.

因其指数为 2,4,4 或 2,24 或 4,14. 为使 n 最小,显然为 $n=5^2\cdot 3^4\cdot 2^4$.

于是 $k=\frac{n}{75}=3^3\cdot 2^4=432$.

7. 证明：设 n 是与集合 S 中任何一个数都不互质的最小正整数（这样的数是存在的，事实上，因为 $1\notin S$，S 中所有数的乘积就与 S 中任何数都不互质）.

在 n 的所有质因子中，每个质数都是一次幂的，否则，n 就不是具有上述性质的最小数，由于数 n 与 S 中任何数都不互质，由题中条件知，存在 $s\in S$，使得 $(s,n)=s$，因此，$s|n$.

设 p 是数 s 的任一个质因子，则 $p|n$. 再由 n 的选取方法可知，数 $\frac{n}{p}$ 与某个 $t\in S$ 互质，由 $\left(t,\frac{n}{p}\right)=1$ 及 $(t,n)>1$，知 $p|t$.

但数 t 不能再被 n 的任何其他质因子整除（因为这些质数都整除 $\frac{n}{p}$），由此可断定，$(s,t)=p$，即 (s,t) 是质数.

8. 证明：因为 p_i 是不小于 5 的素数，则 p_i 仅可表示为 $6k\pm 1$ 型（$k\in\mathbf{N}_+$）. 于是

$p_i^2-1=36k^2\pm 12k=12k(3k\pm 1)$，

由于 k 和 $3k\pm 1$ 的奇偶性不同，所以 $k(3k\pm 1)$ 是偶数，于是 p_i^2-1 能被 24 整除，从而 $p_1^2+p_2^2+\cdots+p_{24}^2-24$ 能被 24 整除.

即 $p_1^2+p_2^2+\cdots+p_{24}^2$ 能被 24 整除.

9. 证明：用数学归纳法证明.

对每个正整数 n，存在唯一的 n 位数 A_n，能被 5^n 整除，其数字均属于集合 $\{1,2,3,4,5\}$.

显然，$A_1=5$，$A_2=25$.

假设 A_n 已定，设 $B_n=\frac{A_n}{5^n}$，则 $n+1$ 位数字 $\overline{C_{n+1}C_n\cdots C_1}=C_{n+1}\cdot 10^n+\overline{C_nC_{n-1}\cdots C_1}$ 能被 5^n 整除，当且仅当 $\overline{C_nC_{n-1}\cdots C_1}$ 能被 5^n 整除.

由归纳假设得

$\overline{C_nC_{n-1}\cdots C_1}=A_n=5^nB_n$.

因此，$\overline{C_{n+1}C_n\cdots C_1}=5^n(2^nC_{n+1}+B_n)$.

当且仅当 $2^nC_{n+1}+B_n$ 能被 5 整除时，该数能被 5^{n+1} 整除.

因为 $(2^n,5)=1$，所以 $2^nx+b\equiv 0\pmod 5$ 在集合 $\{1,2,3,4,5\}$ 中有唯一解，其中 $n\in\mathbf{N}_+$，$b\in\mathbf{N}$.

10. 解：若 $n=pq$，其中 p、q 为不同的质数，则其大于 1 的因数为 p、q、pq，无论怎样放在圆周上，p 和 q 总会相邻，且 p 和 q 互质，不满足要求.

若 $n=p^m$，其中 p 为质数，正整数 $m\geqslant 2$，则无论怎样将 n 的大于 1 的因数放在一个圆

上，任意两个相邻的因数都不互质.

若 $n=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$，其中 $p_1<p_2<\cdots<p_k$，$m_1,m_2,\cdots,m_k$ 为正整数，且 $k>2$ 或 $k=2$ 时，$\max\{m_1,m_2\}>1$.

设 $D_n=\{d\mid d\mid n，且\ d>1\}$.

首先，将 $n,p_1p_2,p_2p_3,\cdots,p_{k-1}p_k$ 按顺时针放在圆上，在 n 和 p_1p_2 之间依任意的次序放入 D_n 中所有以 p_1 为最小质因数的正整数(不包括 p_1p_2)；在 p_1p_2 和 p_2p_3 之间，依任意的次序放入 D_n 中所有以 p_2 为最小质因数的正整数(不包括 p_2p_3)；继续以这种方法放置，最后，在 $p_{k-1}p_k$ 和 n 之间，依任意的次序放入 $p_k,p_k^2,\cdots,p_k^{m_k}$，于是，$D_n$ 中的所有元素恰被放在圆周上一次，且任意相邻的两个数有一个公共的质因数.

因此，这样的安排满足要求.

第二章　同余

§2.1　同余的概念和定义

1. A　提示：易知 $A\leqslant \lg 4568^{7777}\times 9<7777\times 9\times 4=279972$

$B\leqslant 1+5\times 9=46$，

$C\leqslant 3+9=12$.

又 $C\equiv 5(\bmod 9)$，$C\in\mathbf{N}_+$，所以 $C=5$.

2. C　提示：$104=4\times 29-12$，

所以 $104^{2006}\equiv 12^{2006}(\bmod 29)$

$\equiv 144^{1003}(\bmod 29)$

$\equiv(29\times 5-1)^{1003}(\bmod 29)$

$\equiv(-1)^{1003}(\bmod 29)$

$\equiv 28(\bmod 29)$.

3. B　提示：2006! 的末尾的 0 的个数即 5 的指数，而 $L_5(2006!)=\left[\frac{2006}{5}\right]+\left[\frac{2006}{5^2}\right]+\left[\frac{2006}{5^3}\right]+\left[\frac{2006}{5^4}\right]=500$.

4. B　提示：$(2k+1)\cdot(2k+3)\cdot(2k+5)\cdot(2k+7)\equiv 1(\bmod 8)$，

所以 $2005!!\equiv 1\times 3\times 5(\bmod 8)$

$\equiv 7(\bmod 8)$.

而 $125\equiv 5(\bmod 8)$，$375\equiv 7(\bmod 8)$

$625\equiv 1(\bmod 8)$，$875\equiv 3(\bmod 8)$

5. B　提示：$p,p+10,p+14(\bmod 3)$

$=p,p+1,p+2(\bmod 3)$.

又 p 为质数，所以 $p=3$.

又 $p=3$ 是满足要求的.

6. A　提示：若 $p|a$，则 $p|b$，

若 $p\nmid a$，则 $a^{p-1}=(a^2)^{\frac{p-1}{2}}$

$$\equiv(-b^2)^{\frac{p-1}{2}}$$

$$\equiv-b^{p-1}(\bmod p)$$

又 $a^{p-1}\equiv b^{p-1}\equiv1(\bmod p)$（费马小定理），矛盾！

7. 1 或 19　提示：易知 $p\equiv1,7,11,13,17,19,23$ 或 $29(\bmod 30)$.

所以 $p^2\equiv1$ 或 $19(\bmod 30)$.

又 $p=31$ 时，$p^2\equiv1(\bmod 30)$，

$p=67$ 时，$p^2\equiv19(\bmod 30)$.

8. 179　提示：由题意：

$d|1417-1059$　①

$d|2312-1417$　②

所以 $d|2\times179,d|5\times179$.

所以 $d|(2\times179,5\times179)$.

所以 $d|179$，又 $d>1$，179 为质数.

所以 $d=179$.

9. 0　提示：$3333\equiv1(\bmod 7)$，所以 $3333^{8888}\equiv1(\bmod 7)$.

$8888\equiv5(\bmod 7)$，所以 $8888^3\equiv5^3(\bmod 7)\equiv-1(\bmod 7)$.

所以 $8888^{3333}\equiv-1(\bmod 7)$.

10. 1 或 p　提示：如果 $\left(a+b,\dfrac{a^p+b^p}{a+b}\right)=t>1$，设质数 $q|t$，则 $q|a+b$，所以 $a\equiv-b$ $(\bmod q)$.

又 $\dfrac{a^p+b^p}{a+b}=a^{p-1}-a^{p-2}b+\cdots+b^{p-1}$

$$\equiv pa^{p-1}(\bmod q)$$

$$\equiv0(\bmod q).$$

所以 $q|p\cdot a^{p-1}$.

又 $q|a+b,(a,b)=1$，所以 $q\nmid a$，所以 $q|p$. 又 p 为质数，所以 $q=p$.

所以 $t=p^{\alpha}$，若 $\alpha\geqslant2$，易知

$\dfrac{a^p+b^p}{a+b}\equiv p\cdot a^{p-1}(\bmod p^2)\equiv0(\bmod p^2)$.

所以 $p|a \Rightarrow p|b$ 矛盾！所以 $a=1$.

11. 41

提示：$2=|3^1-2^0|$，$3=|3^0-2^2|$，

$5=|3^2-2^2|$，$7=|3^2-2^1|$，

$11=|3^3-2^4|$，$13=|3^1-2^4|$，

$17=|3^4-2^6|$，$19=|3^3-2^3|$，

$23=|3^3-2^2|$，$29=|3^1-2^5|$，

$31=|3^0-2^5|$，$37=|3^3-2^6|$.

再只需证不存在 $m,n\in \mathbf{N}$，满足 $41=|3^m-2^n|$（分两种情况讨论）.

12. 6

提示：$a_0\equiv 1(\bmod 7)$，$a_1\equiv 2(\bmod 7)$，

$a_2\equiv 2^2+1\equiv 5(\bmod 7)$，$a_3\equiv 6(\bmod 7)$，

$a_4\equiv 6(\bmod 7)$，$a_5\equiv 0(\bmod 7)$，

$a_6\equiv 6(\bmod 7)$，$a_7\equiv 1(\bmod 7)$，

$a_8\equiv 2(\bmod 7)$.

所以 $a_{n+7}\equiv a_n(\bmod 7)$，所以 $a_{2006}\equiv a_{7\times 286+4}\equiv a_4\equiv 6(\bmod 7)$.

13. 证明：首先易知 $\sum\limits_{i=1}^{999}|a_i-b_i|\equiv\sum\limits_{i=1}^{999}1(\bmod 5)\equiv 4(\bmod 5)$.

又 $\sum\limits_{i=1}^{999}|a_i-b_i|\equiv\sum\limits_{i=1}^{999}a_i+b_i(\bmod 2)\equiv 1(\bmod 2)$.

所以 $\sum\limits_{i=1}^{999}|a_i-b_i|\equiv 9(\bmod 10)$.

所以和数 $\sum\limits_{i=1}^{999}|a_i-b_i|$ 的末位数为 9.

14. 提示：对 n 用数学归纳法.

15. 证明：(1) 因为 n 为质数，$n|a^n-1$　①

所以 $(a,n)=1$，由费尔马小定理：$a^{n-1}\equiv 1(\bmod n)$，

结合①知 $n|a-1$，即 $a\equiv 1(\bmod n)$，

又 $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots+a+1)$，

而 $a^{n-1}+a^{n-2}+\cdots+a+1\equiv\underbrace{1+1+\cdots+1}_{n个1}(\bmod n)$

$\equiv 0(\bmod n)$，

$n|a-1$，所以 $n^2|(a-1)(a^{n-1}+a^{n-2}+\cdots+a+1)$.

即 $n^2|a^n-1$.

(2) 取 $n=rs$（其中 r,s 为互异的奇质数），

所以 $rs|a^n-1$，所以 $r|a^n-1$，　①

同上知 $r|a^{r-1}-1$ 结合①知 $r|a^s-1$，

所以 $a^n-1=(a^s)^r-1$

$$=(a^s-1)((a^s)^{r-1}+(a^s)^{r-2}+\cdots+a^s+1).$$

易知 $r|a^{s(r-1)}+a^{s(r-2)}+\cdots+a^s+1$，$r|a^s-1$，所以 $r^2|a^n-1$.

同理 $s^2|a^n-1$，又 $(r,s)=1$，所以 $r^2s^2|a^n-1$，即 $n^2|a^n-1$.

又满足 $n=rs$（其中 r,s 为互异奇质数）的 n 显然有无穷多个.

所以(2)得证.

§2.2 完系、简系、剩余类

1. 略

2. 解：设 $A=\{1,2,\cdots,m-1,m\}$，对于 $d|m$，$d\in\mathbf{N}_+$.

设与 d 互质的不大于 d 的正整数分别为 $a_1,a_2,\cdots,a_{\varphi(d)}$，则易知 $\frac{m}{d}\cdot a_1,\frac{m}{d}a_2,\cdots,\frac{m}{d}a_{\varphi(d)}$，即为 s 中与 m 的最大公约数为 $\frac{m}{d}$ 的全部正整数，当 d 取遍 m 的所有约数时，$\frac{m}{d}$ 也取遍 m 的所有约数，于是 s 中每个数在各 $\varphi(d)$ 中算且仅算了一遍.

所以 $s=\sum\limits_{d|m}\varphi(d)=m$.

3. 证明：取 $a_i=3i-2$，$b_i=3i-3\quad(i=1,2,\cdots,n)$，则

$$a_i+a_{i+1}=3i-2+3(i+1)-2=6i-1 \quad ①$$

$$a_i+b_i=3i-2+3i-3=6i-5 \quad ②$$

$$b_i+b_{i+k}=3i-3+3(i+k)-3=6(i-1)+3k \quad ③$$

①、②、③三组数对模 3 不同余，因此模 $3n$ 也不同余，亦即任何来自不同组的两个数被 $3n$ 除所得余数互不相同.

下证同一组内任何两数模 $3n$ 互不同余.

事实上，若存在 p,q，$1\leqslant p<q\leqslant n$，使得

$6(p-1)+r\equiv6(q-1)+r\pmod{3n}\quad(r=1,2$ 或 $3k)$，

则 $6(p-q)\equiv0\pmod{3n}$，所以 $n|2(p-q)$，又 n 为奇数，所以 $p=q$，矛盾！

综上所述，所取 $2n$ 个数 $a_1,a_2,\cdots,a_n,b_1,b_2,\cdots,b_n$ 为符合题目要求的 $2n$ 个整数.

4. 提示：取 $m=\varphi(b)$，$n=\varphi(a)$.

5. 证明：设 $m=17^ip$，$n=17^jq$，其中 $i,j\in\mathbf{N}$，$p,q\in\mathbf{N}_+$，$(p,17)=(q,17)=1$.

下面证明：$p=q$.

设 $p>q$（$p<q$ 的情形可作类似讨论），由于 $(p,17)=1$，由孙子定理知存在 $a\in\mathbf{N}_+$，满足 $a\equiv0\pmod{p}$，$a\equiv-1\pmod{17}$.

于是 $a=17k-1\ (k\in\mathbf{N}_+)$ 且 $(17k-1,m)=(a,17^ip)=p$.

另一方面，由于$(a,17)=1$，所以$(17k-1,n)=(17k-1,17^l q)\leqslant q<p$. 而这与$(17k-1,m)=(17k-1,n)$矛盾！所以 $p=q$.

故存在某个 $l\in \mathbf{Z}$，使得 $m=17^l\cdot n$.

6. 证明：采用反证法. 设这三个数均为完全平方数，则可令

$2d-1=x^2, 5d-1=y^2, 13d-1=z^2$.

从 $2d-1=x^2$ 可知 x 为奇数，因为任何奇数的平方被 8 除余 1，故可设 $x^2=8k+1$，得：

$2d-1=8k+1$，所以 $d=4k+1$，所以 d 为奇数.

从 $5d-1=y^2, 13d-1=z^2$ 知 y,z 均为偶数，两式相减得：$8d=z^2-y^2$.

令 $y=2u, z=2v$，有 $2d=(v-u)(v+u)$.

由于 $v-u$ 与 $v+u$ 具有相同的奇偶性. 又 $2d$ 为偶数，所以 $2\mid v-u, 2\mid v+u$，所以 $4\mid 2d$，所以 $2\mid d$，这与 d 为奇数矛盾！

本题得证.

7. 证明：因为 n 为素数，知对 $k=2,3,\cdots,n$ 均有$(n,k-1)=1$，由孙子定理，存在 b_k 得

$$\begin{cases} b_k\equiv 0 \pmod{k-1}, \\ b_k\equiv k \pmod{n}. \end{cases}$$

设 $a_1=1$，并用 a_k 表示 $c_k=\dfrac{b_k}{k-1}(k\geqslant 2)$ 被 n 除的余数，则 $b_k\equiv c_k(k-1)\equiv a_k(k-1)\pmod{n}$.

(1) 首先证明 $a_n=0$ 且 $k=1,2,\cdots,n-1$ 时，$a_k\neq a_n$.

这是由于 $a_n(n-1)\equiv b_n\equiv n\pmod{n}$，$a_1=1$，$a_k(k-1)\equiv k\pmod{n}$.

(2) 其次证明 $a_l\neq a_k$，$1\leqslant l<k<n$.

否则若 $a_l=a_k=a$，则

$a_l(l-1)k\equiv lk\pmod{n}$，$a_k(k-1)l\equiv kl\pmod{n}$.

即 $a_l(l-1)k-a_k(k-1)l\equiv 0\pmod{n}$，所以$(k-l)a\equiv 0\pmod{n}$. ①

又 n 为质数，则$(a,n)=1$，$(k-l,n)=1$，

所以①式不可能，故 $a_l\neq a_k$.

(3) 最后证 $a_k\neq 1$，$1<k<n$，否则如果 $a_k=1$，则 $b_k\equiv k-1\equiv k\pmod{n}$，矛盾！

由以上知 $a_1,a_2,a_3,\cdots,a_n$ 互不相同，且

$\{a_1,a_2,\cdots,a_n\}=\{0,1,2,\cdots,n-1\}$.

下面证明上述排列是符合要求的.

事实上，由 $a_1=1$，$a_1a_2\cdots a_n=0$，当 $k=2,3,\cdots,n-1$ 时，

$$\begin{aligned} a_1a_2\cdots a_k &\equiv 1\cdot a_2a_3\cdots a_k \equiv 2a_3a_4\cdots a_k \pmod{n} \\ &\equiv 3a_4a_5\cdots a_k \pmod{n} \end{aligned}$$

$\equiv\cdots(\bmod n)$
$\equiv(k-1)a_k(\bmod n)$
$\equiv k(\bmod n)$.

因此 $a_1,a_1a_2,\cdots,a_1a_2\cdots a_n$ 被 n 除的余数集合为$\{1,2,3,4,\cdots,n-2,n-1,0\}$. 证毕.

§2.3 欧拉定理、费马定理、威尔逊定理

1. 解:$k_{\min}=14$ 提示:一方面取 $m=n=1$,则 $k=14$. 另一方面,设 $k=19^n-5^m$.

模 2 可知:$k\equiv0(\bmod 2)$;

模 3 可知:$k\equiv1^n-(-1)^m\equiv0$ 或 $2(\bmod 3)$;

模 5 可知:$k\equiv(-1)^n(\bmod 5)$.

根据以上条件,我们已能判定 $k\neq1,2,3,4,5,7,8,9,10,11,12,13$.

如果 $k=6$,再模 19 得 $5^m\equiv13(\bmod 19)$这是不可能的(可逐一检验 $5^1,5^2,\cdots,5^9$ 分别同余于 5,6,11,17,9,7,16,4,1(mod19)),所以 $k\geqslant14$.

结合两方面知 k 的最小值为 14.

2. 证明:由于 $1,2,3,\cdots,m$ 构成模 m 的完系.

又$(2,m)=1$,所以 $2\times1,2\times2,2\times3,\cdots,2\times m$ 也是模 m 的完系.

所以 $\sum\limits_{k=1}^{m}k^n\equiv\sum\limits_{k=1}^{m}(2k)^n(\bmod m)$.

即 $m\mid(2^n-1)\sum\limits_{k=1}^{m}k^n$,又$(m,2^n-1)=1$,所以 $m\mid\sum\limits_{k=1}^{m}k^n$.

故和数 $1^n+2^n+\cdots+m^n$ 是 m 的倍数.

3. 解:$n\geqslant3$ 时,由 $1000\mid1978^m-1978^n$,得

$125\mid1978^{m-n}-1$,又 $1978=15\times125+103$,

所以 $125\mid103^{m-n}-1$,所以 $25\mid103^{m-n}-1$.

所以 $25\mid3^{m-n}-1$.

记 $m-n=l$,则:$25\mid3^l-1$(显然 l 为偶数,否则易知 $3^l-1\equiv\pm3-1\equiv4$ 或 $2(\bmod 5)$矛盾),记 $l=2a$,

则 $25\mid9^a-1$,又 $9^a-1=(10-1)^a-1$

$$\equiv C_a^2 10^2(-1)^{a-2}+C_a^1 10(-1)^{a-1}+(-1)^a-1(\bmod 25)$$
$$\equiv10a(-1)^{a-1}+(-1)^a-1(\bmod 25)$$

显然 a 为偶数.

所以 $9^a-1\equiv10a(-1)(\bmod 25)$.

所以 $5\mid a$,又 a 为偶数,所以 $10\mid a$.

设 $a=10b$,则 $l=20b$.

所以 $103^l-1=(100+3)^{20b}-1$

$\equiv C_{20b}^{1}100\cdot 3^{20b-1}+3^{20b}-1\pmod{125}$

$\equiv 9^{10b}-1\pmod{125}$

$\equiv(10-1)^{10b}-1\pmod{125}$

$\equiv C_{10b}^{2}\cdot 10^2-C_{10b}^{1}10\pmod{125}$

$\equiv -100b\pmod{125}$，

所以 $5\mid b$，所以 $l=20b\geqslant 100$. 所以 $m+n=l+2n\geqslant 106$.

当 $m=103,n=3$ 上式可取等号.

若 $n\leqslant 2$，易知 $8\nmid 1978^m-1978^n\Rightarrow 1000\nmid 1978^m-1978^n$，所以 $m+n$ 的最小值为 106.

4. 证明：(1) 当 $n\equiv 0\pmod 2$ 时，

$19\cdot 8^n+17\equiv 19+17\pmod 3\equiv 0\pmod 3$.

(2) 当 $n\equiv 1\pmod 4$ 时，设 $n=4k+1$.

$19\cdot 8^{4k+1}+17\equiv 6\times 8\times 64^{2k}+4\pmod{13}$

$\equiv 48+4\pmod{13}\equiv 0\pmod{13}$.

(3) 当 $n\equiv 3\pmod 4$ 时，设 $n=4k+3$.

$19\cdot 8^{4k+3}+17\equiv 4\times 3^3\times 64^{2k}+17\pmod 5$

$\equiv 3+17\pmod 5\equiv 0\pmod 5$.

5. 解：当 $n\geqslant 4$ 时，设 p 是 n 的最小质因数，显然 p 为奇数，$p\mid 2^n+1$，所以 $p\mid 2^{2n}-1$.

又 $p\mid 2^{p-1}-1$ （费马小定理），所以 $p\mid 2^{(2n,p-1)}-1$.

又 $(n,p-1)=1$，所以 $p\mid 2^{(2,p-1)}-1$，所以 $p\mid 3\Rightarrow p=3$.

设 $n=3^k\cdot m(k\in\mathbf{N}_+)$，$(3,m)=1$.

$k\geqslant 2$ 时，$3^{2k}\mid 2^{3^k\cdot m}+1\Rightarrow 3^{k+2}\mid 2^{3^k\cdot m}+1$.

又 $2^{3^k\cdot m}+1=(3-1)^{3^k\cdot m}+1$

$$=\sum_{j=0}^{3^k\cdot m}C_{3^k\cdot m}^{j}3^j(-1)^{3^k\cdot m-j}+1$$

$$=\sum_{j=1}^{3^k\cdot m}C_{3^k\cdot m}^{j}3^j(-1)^{3^k\cdot m-j}.$$

对于 $2\leqslant j\leqslant 3^k\cdot m$.

$$C_{3^k\cdot m}^{j}3^j(-1)^{3^k\cdot m-j}=(-1)^{3^k\cdot m-j}3^j\cdot\frac{3^k\cdot m\cdot(3^k\cdot m-1)\cdots(3^k\cdot m-j+1)}{j!}.$$

$$\text{所以}L_3(C_{3^k\cdot m}^{j}3^j(-1)^{3^k\cdot m-j})\geqslant L_3\left(3^j\,\frac{3^k\cdot m(3^k\cdot m-1)\cdots(3^k\cdot m-j+1)}{j!}\right)$$

$$\geqslant j+k-\sum_{i=1}\left[\frac{j}{3^i}\right]\geqslant k+j-\left(\frac{j}{3}+\frac{j}{3^2}+\cdots+\frac{j}{3^j}\right)$$

$$>k+j-\frac{j}{3}\cdot\frac{1}{1-\frac{1}{3}}=k+\frac{j}{2}\geqslant k+1.$$

所以 $L_3(C_{3^k\cdot m}^{j}3^j(-1)^{3^k\cdot m-j})\geqslant k+2$,(其中 $L_p(a)$ 表示 a 的标准分解式中质数 p 的指数).

所以 $2^{3^k\cdot m}+1\equiv C_{3^k\cdot m}^{1}\cdot 3\pmod{3^{k+2}}\equiv m\cdot 3^{k+1}\pmod{3^{k+2}}\not\equiv 0\pmod{3^{k+2}}$.

所以 $k=1$,于是 $n=3m$(m 为奇数).

又 $n\geqslant 4$,所以 $m>1$,设 q 为 m 的质因数,

则 $q\geqslant 5$,$q|2^{3m}+1\Rightarrow q|2^{6m}-1$,$q|2^{q-1}-1$,

所以 $q|2^{(6m,q-1)}-1=2^{(6,q-1)}-1$.

所以 $q|2^6-1\Rightarrow q|63$,又 $q>3$,所以 $q=7$.

所以 $7|8^m+1$ 矛盾! 所以 $n\leqslant 3$.

经检验 $n=1,3$ 满足要求,$n\neq 2$.

所以满足要求的 n 为 1 或 3.

6. 解:(1)当 p,q 中有一个满足 $a|5^a-2^a$($a=p$ 或 q),不妨设 $p|5^p-2^p$,p 显然不为 2,5,于是 $(p,2)=(p,5)=1$,由费马小定理:$5^{p-1}\equiv 2^{p-1}\equiv 1\pmod p$,所以 $p|3\Rightarrow p=3$.

又 $p\cdot q|(5^p-2^p)(5^q-2^q)$,所以 $3q|9\times 13(5^q-2^q)$,所以 $q=3$ 或 13.

所以此时满足要求的 $(p,q)=(3,13)$ 或 $(3,3)$ 或 $(13,3)$.

(2)当 $p\nmid 5^p-2^p$,$q\nmid 5^q-2^q$,则易知 $p|5^q-2^q$,$q|5^p-2^p$.

不妨 $p\geqslant q$,则 $q|5^p-2^p$, ①

又 $p\geqslant q$,所以 $(p,q-1)=1$,由裴蜀定理,存在 $v\in\mathbf{N}_+$,

满足 $pu-(q-1)v=1$,由①得:

$q|5^{pu}-2^{pu}$,即 $q|5^{(q-1)v+1}-2^{(q-1)v+1}$.

又易知 $5^{q-1}\equiv 2^{q-1}\equiv 1\pmod q$,所以 $q|5-2\Rightarrow q=3$ 与 $q\nmid 5^q-2^q$ 矛盾!

综上所述,符合要求的 $(p,q)=(3,3),(3,13)$ 或 $(13,3)$.

7. 证明:(用反证法)假定存在 $m\in\mathbf{N}_+$,满足 $pq|m^{p-q}+1$,则 $(m,p)=(m,q)=1$,由条件知:$p|m^{p-q}+1\Rightarrow p|m^{p-1}+m^{q-1}$.

又由费尔马小定理 $m^{p-1}\equiv 1\pmod p$,所以 $p|m^{q-1}+1$.

设 $q-1=2^k\cdot\alpha$($k\in\mathbf{N}_+$,$(2,\alpha)=1$),

于是 $p|(m^\alpha)^{2^k}+1\Rightarrow p|(m^\alpha)^{2^{k+1}}-1$. 设 l 是 m 模 p 的阶,则 $l|2^{k+1}$,若 $l\neq 2^{k+1}$,则 $l|2^k$,

所以 $p|l+1$,矛盾! 所以 $l=2^{k+1}$.

又 $p|(m^\alpha)^{p-1}-1$(费尔马小定理),

所以 $2^{k+1}|p-1$,设 $p-1=2^t\cdot\beta$,则 $t>k$.

又 $q|m^{p-1}+m^{q-1}\Rightarrow q|m^{p-1}+1$,

同理有 $2^{t+1}|q-1\Rightarrow k>t$ 与 $t>k$ 矛盾!

原命题得证.

8. 略(本题是例 5 的特殊情形)

9. 解:我们称 n 具有性质 T,如果对所有与 n 互质的整数 a,b,$a\equiv b(\bmod n)$ 当且仅当 $ab\equiv1(\bmod n)$. 不难发现 n 具有性质 T 亦可等价于对任意 $a\in\mathbf{Z}$,若 $(a,n)=1$,则 $a^2\equiv1(\bmod n)$. 我们将证明:若 n 具有性质 T,则 n 的任一质因数亦具有性质 T.

事实上,对任意 $a\in\mathbf{Z}$,如果 $(a,p)=1$,则存在 $a'\in\mathbf{Z}$,$(a,a')=1$ 且 $a\equiv a'(\bmod p)$,于是

$a^2\equiv(a')^2(\bmod p)$,$(a')^2\equiv1(\bmod n)$,

所以 $(a')^2\equiv1(\bmod p)\Rightarrow a^2\equiv1(\bmod p)$.

由 a 的选取方式,可知 p 具有性质 T.

下面考虑具有性质 T 的质数 p,若 $p\geqslant5$,则 $(2,p)=1$,而 $2^2\not\equiv1(\bmod p)$,则 p 不具有性质 T. 故 p 只能为 2 或 3.

于是可得具有性质 T 的正整数 n 必然具有 $2^\alpha\cdot3^\beta(\alpha,\beta\geqslant0)$ 的形式,故可取 $(5,n)=1$. 所以 $n\mid5^2-1=24$.

所以具有性质 T 的大于 1 的正整数只可能为:2,3,4,6,8,12,24.

经检验,上面这 7 个自然数的确具有性质 T,它们即为所求.

10. 解:容易验证 $p=2,3,5,7$ 均满足条件,现在讨论 $p\geqslant11$,若 p 满足条件,则:

(1) $p-4$ 没有大于 4 的质因数;

(2) $p-8$ 没有大于 8 的质因数;

(3) $p-9$ 没有大于 9 的质因数.

由(1)得:$p-4=3^a(a\geqslant2)$ ①

由上式及 $p-8$ 是奇数知 $p-8$ 不能被 2 和 3 整除. 因此由(2)知,$p-8=5^b\cdot7^c$ ②

由①,②得 $5^b7^c-3^a+4=0(a\geqslant2)$ ③

上式两边取模 3 得 $(-1)^b+1=0\Rightarrow1\leqslant b=2l+1,l\geqslant0$.

由于 $b\geqslant1$ 由式③推出 $5\mid3^a+1\Rightarrow2\leqslant a=4m+2\quad(m\geqslant0)$.

由式②知 $p-q=5^b\cdot7^c-1$,则 $p-q$ 不能被 3 整除.

由于 $b\geqslant1$,所以也不能被 5 整除.

下面来证明:$c=0$.

若不然设 $c\geqslant1$,设 $7\nmid p-q$. 由此及③知

$p-q=5^b\cdot7^c-1=2^d\quad(c\geqslant1)\Rightarrow7\mid2^d+1$,这是不可能的.

由式①,②及 $c=0$ 得

$5^b=3^a-4=(3^{2m+1}-2)(3^{2m+1}+2)$.

设 $(3^{2m+1}-2,3^{2m+1}+2)=g$,显见 g 为奇数且 $g\mid4$,所以 $g=1$.

由此知 $3^{2m+1}-2=1, 3^{2m+1}+2=5^b$，所以 $m=0, b=1, a=2$.

所以由式①知，满足条件的质数仅有 13.

综上所述，满足本题条件的全部质数是：2，3，5，7，13.

11. 解：由条件知 $x|yz-2, z|xy-2, y|xz-2$，

则 $xyz|(yz-2)(xy-2)(xz-2)$，

又 $(xy-2)(xz-2)(yz-2)=x^2y^2z^2-2(x^2yz+xy^2z+xyz^2)+4(xy+xz+yz)-8$，所以 $xyz|4(xy+xz+yz)-8$.

设 $4(xy+xz+yz)-8=kxyz$，则 $4\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)=k+\frac{8}{xyz}$.

由条件知 $x、y、z>2$，若 $x、y、z$ 中有两个数相等. 不妨设 $x=y$，则 $yz\equiv 0(\bmod x)$，矛盾！所以 x,y,z 互不相等.

不妨设 $x\leqslant y\leqslant z$，则 $4\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)\leqslant 4\left(\frac{1}{3}+\frac{1}{4}+\frac{1}{5}\right)<4$，故 $k\leqslant 3$.

(1) 若 $k=3$，如果 $x\geqslant 4$，则

$4\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)\leqslant 4\left(\frac{1}{4}+\frac{1}{5}+\frac{1}{6}\right)<3$，矛盾.

所以 $x=3$. 如果 $y\geqslant 5$，则

$4\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)\leqslant 4\left(\frac{1}{3}+\frac{1}{5}+\frac{1}{6}\right)<3$，矛盾！所以 $y=4$.

所以 $4\left(\frac{1}{3}+\frac{1}{4}+\frac{1}{z}\right)=3+\frac{8}{12z}\Rightarrow z=5$，经检验不满足要求(舍去).

(2) 若 $k=2$，则 $2\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)=1+\frac{4}{xyz}\Rightarrow (x-2)yz-2x(y+z)+4=0$.

如果 $x\geqslant 6$，则 $2\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)\leqslant 2\left(\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)<1$，矛盾！

所以 $3\leqslant x\leqslant 5$.

(ⅰ) $x=3$ 时，解得 $(x,y,z)=(3,7,38),(3,8,22),(3,10,14)$，经检验 $(x,y,z)=(3,8,22),(3,10,14)$ 满足题设要求.

(ⅱ) $x=4$ 时，解得 $(x,y,z)=(4,5,18),(4,6,11)$，经检验，均满足题设要求.

(ⅲ) $x=5$ 时，解得 $(x,y,z)=(5,6,7)$，经检验，不满足题设要求.

(3) 若 $k=1$，则

$4\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)=1+\frac{8}{xyz}\Rightarrow (-4+x)yz-4x(y+z)+8=0$.

若 $x\leqslant 4$，则 $\frac{4}{x}\geqslant 1, \frac{4}{y}\geqslant\frac{4}{xyz}, \frac{4}{z}>\frac{4}{xyz}$，于是

$\frac{4}{x}+\frac{4}{y}+\frac{4}{z}>1+\frac{8}{xyz}$，矛盾！

若 $x\geqslant 12$，则

$4\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)\leqslant 4\left(\frac{1}{12}+\frac{1}{13}+\frac{1}{14}\right)<1$，矛盾！

所以 $5\leqslant x\leqslant 11$.

(ⅰ) $x=5$，解得 $(x,y,z)=(5,21,412),(5,22,216),(5,24,118),(5,28,69),(5,27,76),(5,34,48)$，经检验均不满足要求.

(ⅱ) $x=6$，代入解得 $(x,y,z)=(6,13,152),(6,14,82),(6,16,47),(6,17,40),(6,19,32),(6,22,26)$，经检验 $(6,14,82),(6,22,26)$ 满足要求.

(ⅲ) $x=7$，解得 $(x,y,z)=(7,10,136),(7,11,60),(7,12,41),(7,16,22)$，经检验均不满足要求.

(ⅳ) $x=8$ 时，解得 $(x,y,z)=(8,9,70),(8,10,39)$，经检验均不满足要求.

重复上述过程，易知当 $x=9,10,11$ 均不满足要求.

综上所述满足条件的 (x,y,z) 是 $(3,8,22),(3,10,14),(4,5,18),(4,6,11),(6,14,82),(6,22,26)$ 以及和它们对称的数组.

12. 证：记 $f(x)=(xp-1)(xp-2)\cdots(xp-p+1)(x\in\mathbf{N}_+)$，

则 $C_{ap}^{bp}=\frac{ap\cdot(ap-p)\cdots(ap-bp+p)}{bp(bp-p)\cdots 2p\cdot p}\cdot\frac{f(a)f(a-1)\cdots f(a-b+1)}{f(b)f(b-1)\cdots f(1)}$

$=C_a^b\frac{f(a)f(a-1)\cdots f(a-b+1)}{f(b)f(b-1)\cdots f(2)f(1)}$，

故只需证：$f(a)f(a-1)\cdots f(a-b+1)\equiv f(b)f(b-1)\cdots f(2)f(1)\pmod{p^3}$ ①

下面证明如下引理：$f(x)\equiv(p-1)!\pmod{p^3}$，$\forall x\in\mathbf{Z}$.

事实上，记 $\delta_0=1$，以及将 $k\geqslant 1$ 时，$\delta_k=\sum\limits_{1\leqslant i_1<i_2<\cdots<i_k\leqslant p-1} i_1\cdot i_2\cdots i_k$.

则由韦达定理：

$f(xp)=\sum\limits_{k=0}^{p-1}(xp)^k(-1)^{p-1-k}\delta_{p-1-k}\equiv\delta_{p-1}-\delta_{p-2}xp+x^2p^2\cdot\delta_{p-3}\pmod{p^3}$.

下面证明：$p\mid\delta_{p-3}$，$p^2\mid\delta_{p-2}$. ②

如果 $s\equiv tr\pmod m$，且 $(m,t)=1$，则简记 $\frac{s}{t}\equiv r\pmod m$.

设 $\frac{s_1}{t_1}\equiv r_1\pmod m$，$\frac{s_2}{t_2}\equiv r_2\pmod m$.

不难证明：$\frac{s_1}{t_1}+\frac{s_2}{t_2}\equiv r_1+r_2\pmod m$.

且若 $s_1\equiv s_2\pmod m$，$t_1\equiv t_2\pmod m$，则 $r_1\equiv r_2\pmod m$.

在上述定义中，下面证明②

$$\delta_{p-3}=(p-1)!\sum_{1\leqslant i<j\leqslant p-1}\frac{1}{ij}\equiv(p-1)!\sum_{1\leqslant i<j\leqslant p-1}i^{-1}j^{-1}(\bmod p)$$

$$\equiv\frac{(p-1)!}{2}\sum_{i\neq j}i^{-1}j^{-1}(\bmod p)\equiv\frac{(p-1)!}{2}\sum_{s\neq t}st(\bmod p)$$

$$\equiv\frac{(p-1)!}{2}\left\{\left[\frac{p(p-1)}{2}\right]^2-\frac{(p-1)p(2p-1)}{6}\right\}(\bmod p)$$

$\equiv 0(\bmod p)$.

$$\delta_{p-2}=(p-1)!\sum_{i=1}^{p-1}\frac{1}{i}=p!\sum_{i=1}^{\frac{p-1}{2}}\frac{1}{i(p-i)},\qquad ③$$

而 $\sum\limits_{i=1}^{\frac{p-1}{2}}\frac{1}{i(p-i)}\equiv\sum\limits_{i=1}^{\frac{p-1}{2}}-(i^{-1})^2(\bmod p)$，

容易证明，对每一个 $1\leqslant i\leqslant\frac{p-1}{2}$，存在唯一的 $1\leqslant j\leqslant\frac{p-1}{2}$，使得 $(i^{-1})^2\equiv j^2(\bmod p)$，

所以 $\sum\limits_{i=1}^{\frac{p-1}{2}}\frac{1}{i(p-i)}\equiv\sum\limits_{j=1}^{\frac{p-1}{2}}(-j^2)(\bmod p)\equiv-\frac{p(p^2-1)}{24}(\bmod p)$，

代入③知 $p^2\mid\delta_{p-2}$，于是②得证.

由引理马上得知，左边和右边模 p^3 均同余于 $[(p-1)!]^b$，故①成立.

从而原命题得证.

13. 证明：先证必要性，设存在 $a\in\mathbf{Z}$，$a^2\equiv-1(\bmod p)$，则

$(-1)^{\frac{p-1}{2}}\equiv a^{p-1}(\bmod p)\equiv 1(\bmod p)$（费尔马小定理），

所以 $p\equiv 1(\bmod 4)$.

再证充分性. 若 $p\equiv 1(\bmod 4)$，即 $2\left|\frac{p-1}{2}\right.$. 于是

$$\begin{aligned}(p-1)!&=1\times2\times\cdots\times\frac{p-1}{2}\times(p-1)\cdot(p-2)\cdots\left(p-\frac{p-1}{2}\right)\\&\equiv1\times2\times\cdots\times\frac{p-1}{2}\times(-1)(-2)\cdots\left(-\frac{p-1}{2}\right)(\bmod p)\\&\equiv(-1)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2(\bmod p)\\&\equiv\left[\left(\frac{p-1}{2}\right)!\right]^2(\bmod p),\end{aligned}$$

从而由威尔逊定理

$$\left[\left(\frac{p-1}{2}\right)!\right]^2\equiv(p-1)!\equiv-1(\bmod p).$$

14. 证明：(1) $\frac{1}{p}$ 的最小循环节的长度是满足 10^d-1 可以被 p 整除的最小整数 $d(d\geqslant 1)$.

设 q 是质数，$N_q=10^{2q}+10^q+1$，则 $N_q\equiv 3(\bmod q)$，设 p_q 是 $\frac{N_q}{3}$ 的一个质因子，则 p_q 不能被 3 整除，因为 N_q 是 $10^{3q}-1$ 的因子，$\frac{1}{p_q}$ 的循环节长度为 $3q$，所以 $\frac{1}{p_q}$ 的最小循环节的长度是 $3q$ 的因子，若最小循环节的长度为 q，则由 $10^q\equiv 1(\bmod p_q)$ 得 $N_q\equiv 10^{2q}+10^q+1(\bmod p_q)$，矛盾！若最小循环节的长度为 3，只能有一种情况即 p_q 是 $10^3-1=3^3\times 37$ 的因子，即 $p_q=37$. 此时 $N_q=3\times 37\equiv 3(\bmod 4)$，而 $N_q=10^{2q}+10^q+1\equiv 1(\bmod 4)$ 矛盾！于是，对每个素数 q，我们能找到一个质数 p_q，使得 $\frac{1}{p_q}$ 的小数部分的最小循环节的长度为 $3q$.

(2) 设质数 $p\in S$，$3r(p)$ 是 $\frac{1}{p}$ 的最小循环节的长度，p 是 $10^{3r(p)}-1$ 的因子，但不是 $10^{r(p)}-1$ 的因子，所以，p 是 $N_r=10^{2r(p)}+10^{r(p)}+1$ 的因子.

设 $\frac{1}{p}=0.\overline{a_1a_2\cdots}$，$x_j=\frac{10^{j-1}}{p}$，$y_j=\{x_j\}=0.\overline{a_ja_{j+1}\cdots}$，其中 $\{x\}$ 表示 x 的小数部分，则 $a_j<10y_j$. 于是 $f(k,p)=a_k+a_{k+r(p)}+a_{k+2r(p)}<10(y_k+y_{k+r(p)}+y_{k+2r(p)})$，由于 $x_k+x_{k+r(p)}+x_{k+2r(p)}=\frac{10^{k-1}\cdot N_{r(p)}}{p}$ 是整数，所以 $y_k+y_{k+r(p)}+y_{k-2r(p)}$ 也是整数且是小于 3 的数，所以 $y_k+y_{k-r(p)}+y_{k-2r(p)}\leqslant 2$，所以 $f(k,p)<20$，所以 $f(k,p)\leqslant 19$，由于 $f(2,7)=4+8+7=19$，故所求的最大值为 19.

15. 解：对于 $h=2^r$，若是将满足条件的所有 k 的集合记为 $k(h)$，我们来证明：

$k(h)=\{2^{r+s}\cdot t\mid s,t\in\mathbf{N},2\nmid t\}$，

将用到以下事实：$m\equiv 1(\bmod 4)\Rightarrow 2^r\left|\frac{m^{2^r}-1}{m-1}\right.$，

这个事实是显然的，因为

$\frac{m^{2^r}-1}{m-1}=(m^{2^{r-1}}+1)(m^{2^{r-2}}+1)\cdots(m^2+1)(m+1)$.

(1) 先证：若 $s\geqslant 2$，$2\nmid t$，则 $k=2^{r+s}t\in k(h)$.

事实上，存在 $m=2^s\cdot t+1$，$n=m-1$，使得我们有 $2^r\left|\frac{m^{2^r}-1}{m-1}\right.$.

$\frac{m^h-1}{k}=\frac{m^{2^r}-1}{2^{r+s}t}=\frac{m^{2^r}-1}{2^r(m-1)}$ 是奇自然数.

所以 $k\mid m^h-1$.

又 $n^{\frac{m^h-1}{k}}=(m-1)^{\frac{m^h-1}{k}}\equiv -1(\bmod m)$，所以 $m\mid n^{\frac{m^h-1}{k}}+1$.

(2)再证：对于 $2\nmid t$，$k=2^{r+1}t\in k(h)$.

事实上，存在 $m=4t^2+1$，$n=2t$，使我们有

$\frac{m^h-1}{k}=\frac{m^{2^r}-1}{2^r(m-1)}\cdot 2t$，$n^{\frac{m^h-1}{k}}=(n^2)^{\frac{m^{2^r}-1}{2^r(m-1)}\cdot t}\equiv -1(\bmod m)$.

(3)用反证法论证：对于 $0\leqslant q\leqslant r$，$2\nmid t$，$2^q\cdot t\notin k(h)$，若对 $k=2^q\cdot t$ 有 m，n 满足题目中所述的要求，显然有 $(m,n)=1$，在 m 的所有素因数中取以下表示中指数 a 最小的一个素数 p：

$p=2^a\cdot b+1$，$2\nmid b$，易见 $2^a\mid m-1$.

一方面 $p\mid n^{\frac{m^h-1}{k}}+1$，我们有

$(n^{\frac{m^h-1}{2^q\cdot t}})^b=(n^{\frac{m^h-1}{2^{q+a}\cdot t}})^{2^a\cdot b}\equiv(n^{\frac{m^h-1}{2^{q+a}\cdot t}})^{p-1}\equiv 1(\bmod p)$（费马小定理），矛盾！

所以 $k(h)=\{2^{r+s}t\mid s\in\mathbf{N}_+,t\in\mathbf{N},2\nmid t\}$.

第三章　同余方程与平方剩余

§3.1　一次同余方程与孙子定理

1. 对于方程组(Ⅰ)，先解②，得 $x\equiv -1,3(\bmod 8)$，所以(1)的解即下面两个同余方程组的解 $x\equiv 3(\bmod 7)$，$x\equiv -1(\bmod 8)$，或 $x\equiv 3(\bmod 7)$，$x\equiv 3(\bmod 8)$

利用中国剩余定理知(Ⅰ)的解为 $x\equiv 3,31(\bmod 56)$

对于方程组(Ⅱ)，它和下面的同余方程组同解

$$\begin{cases}3x\equiv 1(\bmod 2),\\3x\equiv 1(\bmod 5),\\4x\equiv 7(\bmod 3),\\4x\equiv 7(\bmod 5).\end{cases}$$

但由 $3x\equiv 1(\bmod 5)\Rightarrow x\equiv 2(\bmod 5)$，

由 $4x\equiv 7(\bmod 5)\Rightarrow x\equiv 3(\bmod 5)$，矛盾！

故方程组(2)无解.

2. 利用中国剩余定理，考虑同余方程组：$x\equiv -j+1(\bmod p_j^3)$，其中 $j=1,2,\cdots,k$，p_1，p_2，$\cdots$，p_k 是两两不同的质数.

3. 和上题类似，以 a_j 代替 2 中的 p_j.

4. 我们只需证明存在 n 个连续正整数，其中每个数至少有一个素因子，在这个数的标准分解式中仅出现一次，我们选取 n 个互不相同的素数 $p_1,p_2,\cdots,p_n$，考虑同余方程组 $x\equiv -i+p_i(\bmod p_i^2)$，$i=1,2,\cdots,n$.

由中国剩余定理，上述同余方程组有解．对 $1\leqslant i\leqslant n$，由 $p_i^2\mid p_i-(x+i)\Rightarrow p_i\mid x+i$．又 $p_i^2\nmid x+i$，即 p_i 在 $x+i$ 的标准分解式中恰出现一次．

5. 取 $2n$ 个互不相同的素数 $p_1,p_2,\cdots,p_{2n}$，由中国剩余定理知，同余方程组 $x\equiv -k\pmod{p_{2k-1}p_{2k}}$，$k=1,2,\cdots,n$ 有解．因对任意 k，$x+k$ 至少有两个不同的素因子，从而它不可能为一个素数的幂．

6. (1) $n=2^m$ 时，$\sum\limits_{k=1}^{2n-1}k=\dfrac{(2n-1)\cdot 2n}{2}=(2^{m+1}-1)\cdot 2^m$，一方面 2^m 能整除上式，另一方面，若 $r\leqslant 2n-2$，则 $\sum\limits_{k=1}^{r}k=\dfrac{r(r+1)}{2}$ 不能被 2^m 整除，这是因为 r 和 $r+1$ 中有一个为奇数，另一个不超过 $(2n-2)+1=2^{m+1}-1$．由这两方面，即知 $f(2^m)=2^{m+1}-1$．

(2) 当 n 不是 2 的方幂时，设 $n=2^m a$，其中 $m\geqslant 0$，$a>1$ 为奇数．我们证明，存在正整数 $r<2n-1$，使 $2^{m+1}\mid r$，且 $a\mid r+1$，于是 $\sum\limits_{k=1}^{r}k=\dfrac{r(r+1)}{2}$ 被 $2^m\cdot a=n$ 整除，因而 $f(n)<2n-1$．

为证明上述断定，考虑 $x\equiv 0\pmod{2^{m+1}}$，$x\equiv -1\pmod{a}$，由 $(a,2^{m+1})=1$，故上同余方程组必有解 x_0，并且全部解为 $x\equiv x_0\pmod{2^{m+1}a}$．进一步，由第二个方程知 $r\neq 2n$，由第一个方程知 $0\leqslant r<2n-1$，这便证明了满足要求的 r．

7. 我们先证明，当 n 为素数的幂 p^a 时结论成立．实际上，能够证明，存在 x,y 使 $p\nmid xy$，且 $x+y=k$．

若 $p=2$，则条件表明 k 为偶数，此时可取 $x=1,y=k-1$；若 $p>2$，则 $x=1,y=k-1$ 或 $x=2,y=k-2$ 中有一对满足要求．

一般情况下，设 $n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ 是 n 的标准分解式，上面已证明，对每个 p_i，均存在整数 x_i,y_i，使得 $p_i\nmid x_iy_i$，且 $x_i+y_i=k\ (i=1,2,\cdots,r)$．而由中国剩余定理，同余方程组

$$x\equiv x_i\pmod{p_i^{a_i}}\ (i=1,2,\cdots,r) \qquad ①$$

有解．同余方程组

$$y\equiv y_i\pmod{p_i^{a_i}}\ (i=1,2,\cdots,r) \qquad ②$$

有解．

由 $p_i\nmid x_iy_i$，故 $p_i\nmid xy\ (i=1,2,\cdots,r)$，所以 $(xy,n)=1$．

又由①②知，$x+y\equiv x_i+y_i\equiv k\pmod{p_i^{a_i}}\ (i=1,2,\cdots,r)$，所以 $x+y\equiv k\pmod{n}$．

8. 事实是，对任意的 n，都存在 m 使得 $2^{2^n}-1\mid m^2+9$．

由 $2^{2^k}-1=(2^{2^{k-1}}+1)(2^{2^{k-1}}-1)=(2^{2^{k-1}}+1)(2^{2^{k-2}}+1)(2^{2^{k-2}}-1)$

$=(2^{2^{k-1}}+1)(2^{2^{k-2}}+1)\cdots(2^2+1)(2+1)$．

同余方程 $x^2\equiv -1\pmod{2^{2^n}+1}$ 有解 $x\equiv 2^{2^{n-1}}\pmod{2^{2^n}+1}$，

而 $j>i$ 时，$(2^{2^i}+1,2^{2^j}+1)=(2^{2^{i+1}}-1,2^{2^j}+1)=(2^{2^{i+2}}-1,2^{2^j}+1)=\cdots=(2^{2^j}-1,$

$2^{2^j}+1)=1$，所以，根据中国剩余定理，同余方程组

$x\equiv 2^{2^{n-1}}(\bmod 2^{2^n}+1)$，$n=1,2,\cdots,k-1$，有解 x_0.

令 $m=3x_0$，则满足题中要求.

即对任意的 n，都存在 m 使得 $2^{2^n}-1\mid m^2+9$.

9. 采用反证法，假定命题不成立，即存在整数 x_i，使得 $F(x_i)$ 不是 a_i 的倍数，$i=1,2,\cdots,m$. 于是存在整数 $d_i=p_i^{a_i}(i=1,2,\cdots,m)$，其中 p_i 为质数，α_i 为正整数，使得 a_i 能被 d_i 整除，但 $F(x_i)$ 却不能被 d_i 整除. 在 $d_1,d_2,\cdots,d_m$ 中如果存在有同一质数的方幂，则仅保留其中幂次最高，去掉那些幂次较高的，这样就得到一个两两互质的数组，不妨设为 $d_1,d_2,\cdots,d_s$.

由中国剩余定理知，存在整数 N，使得 $N\equiv x_i(\bmod d_i)$，$i=1,2,\cdots,s$. 又因为 $F(x)$ 为整系数多项式，所以 $F(x)-F(y)$ 能够被 $x-y$ 整除，从而 $F(N)$ 不能被 $d_1,d_2,\cdots,d_s$ 整除，由 $d_1,d_2,\cdots,d_s$ 的选取即知 $F(N)$ 也不能被 $d_1,d_2,\cdots,d_m$ 整除，因此也不能被 $a_1,a_2,\cdots,a_m$ 中任何一个数整除，与已知矛盾！故原命题成立.

10. 设 $p_{i,j}$ 表示 $(2n+1)^2$ 个互不相同的素数，$-n\leqslant i,j\leqslant n$，则同余方程组 $x\equiv i(\bmod p_{i,j})$，$-n\leqslant i,j\leqslant n$.

及 $y\equiv i(\bmod p_{i,j})$，$-n\leqslant i,j\leqslant n$，均是有解 $x=a,y=b$ 的.

若有一个既约整点 (x',y') 与 (a,b) 之间距离 $\leqslant n$，则可设 $a-x'=i,b-y'=j$. 其中 $-n\leqslant i,j\leqslant n$，即 $x'=a-i,y'=b-j$，但 $p_{i,j}\mid a-i,p_{i,j}\mid b-j$，从而整点 (x',y') 不是既约整点.

§3.2 平方剩余

1. 注意到此时 j 和 $p-j$ 必同为二次剩余或二次非剩余，$1\leqslant j\leqslant\frac{p-1}{2}$，利用定理 1，可以证明.

2. 设 $j^2=pq_j+r_j$，$1\leqslant r_j<p$，$1\leqslant j\leqslant\frac{p-1}{2}$，由此及 $q_j=\left[\frac{j^2}{p}\right]$ 即得 $S=\sum r_j=\sum j^2-p\sum\left[\frac{j^2}{p}\right]$.

利用上一题中的(3)即得

$$S=\frac{p(p^2-1)}{24}-p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{j^2}{p}\right].$$

3. 注意到 m^2+9 的质因子除去 3 外，都应是 $4k+1$ 型的质数，这是因为若 p 是 m^2+9 的质因子，则 $\left(\frac{-9}{p}\right)=1$，或 $p=3$.

设 $n=2^s\cdot t$，t 为奇数. 若 $t>1$，则 $2^t-1\mid 2^n-1\mid m^2+9$.

注意到 $2^t-1\equiv(-1)^t-1\equiv-2(\bmod 3)$，即 2^t-1 不是 3 的倍数，从而 2^t-1 的质因子必全为 $4k+1$ 型，否则有质数 $p\equiv1(\bmod 4)$，$p\mid m^2+9$，矛盾.

而 $2^t-1\equiv-1(\bmod 4)(t>1)$，即 $-1\equiv2^t-1\equiv1\cdot1\cdot\cdots\cdot1\equiv1(\bmod 4)$，矛盾. 从而必有 $t=1$，即 $n=2^s$.

下面的证明即上一节"能力训练"习题 8.

4. 利用反证法，若 $p\nmid a$，则由 $p\mid a^2+b^2$，得 $p\nmid b$，从而存在 b 使得 $a^2\equiv-b^2(\bmod p)\Leftrightarrow-1$ 是模 p 的二次剩余 $\Leftrightarrow p\equiv1(\bmod 4)$，矛盾.

5. 首先证明，对任给的 k，存在一个正整数 a_k，满足 $a_k^2\equiv-7(\bmod 2^k)$，关于 k 用数学归纳法进行证明.

直接观察表明，当 $k\leqslant3$ 时，取 $a_k=1$ 便可满足条件，设对某个 $k>3$，我们有 $a_k^2\equiv-7(\bmod 2^k)$.

下面考虑 a_k^2 模 2^{k+1} 的值，它或者为 $a_k^2\equiv-7(\bmod 2^{k+1})$ 或者为 $a_k^2\equiv2^k-7(\bmod 2^{k+1})$，对于前者，可取 $a_{k+1}=a_k$，对于后者，可取 $a_{k+1}=a_k+2^{k-1}$. 这是由于 $k\geqslant3$，及 a_k 为奇数，所以 $a_{k+1}^2\equiv a_k^2+2^ka_k+2^{2k-2}\equiv a_k^2+2^k\equiv-7(\bmod 2^{k+1})$.

上式的推出利用了归纳假设.

最后，容易看出，序列 $\{a_k\}$ 没有最大元素，因而可要求对任何正整数 k，$a_k^2\geqslant2^k-7$. 因而 $\{a_k\}$ 包含了无穷多个不同的值，因而命题成立.

6. 若方程有正整数解 x,y，方程两边同乘以 4，得 $4(x^2+3xy-2y^2)=488$.

即 $(4x^2+12xy+9y^2)-17y^2=17\times29-5$，

所以 $(2x+3y)^2\equiv-5(\bmod 17)$. ①

只需注意 -5 不是模 17 的二次剩余，所以①式无解. 所以原方程无解.

7. 用反证法：方程 $3y^2=(x^3+1)x$ 有一组整数解 x、y，由 x 与 x^3+1 是互质的，即存在正整数 u,v，使得 $y=u\cdot v$，且 $3u^2=x^3+1$，$v^2=x$ 或 $u^2=x^3+1$，$3v^2=x$.

前一种情况显然不可能，现假定后一种情况成立.

注意到，这时 $u^2=(x+1)(x^2-x+1)$.

由于 $x\equiv0(\bmod 3)$，而 $x^2-x+1=(x+1)(x-2)+3$.

又 $x+1$ 与 x^2-x+1 是互质的，因此，存在 t 满足 $x^2-x+1=t^2$，容易看出，方程 $x^2-x+1=t^2$ 只有一个正整数 $x=1$，但这与 $x\equiv0(\bmod 3)$ 矛盾.

因此，题目结论成立.

8. 对于(1)，我们可利用欧拉判别法证明：$x_0=\pm a^{m+1}$ 是 $x^2\equiv a(\bmod p)$ 的解. 对于(2)，我们利用欧拉判别法及 $\left(\dfrac{-2}{p}\right)=-1$. 解的形式可分开来写：

当 $a^{2m+1}\equiv1(\bmod p)$ 时，$x_0\equiv\pm a^{m+1}$，

当 $a^{2m+1}\equiv -1(\mathrm{mod}\,p)$ 时，$x_0\equiv \pm 2^{2m+1}a^{m+1}$.

注：$\left(\frac{-2}{p}\right)=(-1)$ 的证明需要用到 Gauss 引理，可查看有关书籍.

9. 假设这样的素数只有有限多个，设它们为 $p_1,p_2,\cdots,p_k$.

我们考虑 $(2p_1\cdots p_k)^2+1=p$，由假设及 $p\equiv 1(\mathrm{mod}4)$，所以 p 不是素数，设 p_0 是 p 的素因子，p_0 当然是奇数，所以 -1 是模 p_0 的二次剩余，即 $\left(\frac{-1}{p_0}\right)=1$，从而 $p_0\equiv 1(\mathrm{mod}4)$，但 p_0 显然不是 $p_1,p_2,\cdots,p_k$，这和假设矛盾.

所以形如 $4k+1$ 的素数有无穷多个.

10. 首先不加证明的指出 $\left(\frac{2}{p}\right)=1\Leftrightarrow p\equiv 1(\mathrm{mod}8)$，设 p 是 x^4+1 的奇素因数，即 $(x^2)^2\equiv x^4\equiv -1(\mathrm{mod}\,p)$，由 $\left(\frac{-1}{p}\right)=1$，推出 $p\equiv 1(\mathrm{mod}4)$.

而另一方面 $x^4+1=(x^2+1)^2-2x^2$，所以有 $(x^2+1)^2\equiv 2x^2(\mathrm{mod}\,p)$.

由 $(p,2x)=1$，利用 Legendre 符号的性质

$1=\left(\frac{(x^2+1)^2}{p}\right)=\left(\frac{2x^2}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{x^2}{p}\right)=\left(\frac{2}{p}\right)$.

从而推出 $p\equiv \pm 1(\mathrm{mod}8)$.

而由 $p\mid x^4+1$，从而必有 $p\equiv 1(\mathrm{mod}8)$.

下面证明原命题，若这样的素数只有有限个，设为 $p_1,p_2,\cdots,p_k$. 考虑 $p=(2p_1p_2\cdots p_k)^4+1$，由假设及 $p\equiv 1(\mathrm{mod}8)$ 知 p 不是素数，设 p_0 是 p 的素因子，当然 p_0 是奇数.

由已证结论知 $p_0\equiv 1(\mathrm{mod}8)$，但 p_0 不是 $p_1,p_2,\cdots,p_k$ 中的任一个，矛盾.

所以，有无限多个 $8k+1$ 型的素数.

第四章　不定方程(组)

§4.1　公式法解不定方程

1. A　因 $(903,731)=43$，而 $43\nmid 1106$.

2. A　可求得方程的全部整数解为

$$\begin{cases}x=-30+97t,\\ y=40-96t\end{cases}\quad (t\in\mathbf{Z})$$

令 $x,y\geqslant 0$，得 $\frac{30}{97}\leqslant t\leqslant\frac{40}{96}$，$t$ 无整数取值.

故方程无非负整数解.

3. 证：首先证明当 $a_1,b_1,c_1\in\mathbf{N}_+$，$(a_1,b_1)=1$ 时，不定方程 $a_1x+b_1y=c_1$ 有非负整数解的充分条件是 $c_1>a_1b_1-a_1-b_1$.　①

由裴蜀定理知必有 x_0,y_0 使得 $a_1x_0+b_1y_0=1(x_0,y_0\in\mathbf{Z})$，则知 $a_1x+b_1y=c_1$ 是有整数解的，任取其中一对整数解 x_1,y_1，则其所有整数解由

$$\begin{cases}x=x_1+b_1t,\\y=y_1-a_1t\end{cases}\quad(t\in\mathbf{Z})$$

给出，令 $x\geqslant0,y\geqslant0$ 得 $-\frac{x_1}{b_1}\leqslant t\leqslant\frac{y_1}{a_1}$.

于是 $-\left[\frac{x_1}{b_1}\right]\leqslant t\leqslant\left[\frac{y_1}{a_1}\right]$（这里 $[x]$ 表示不超过 x 的最大整数）.

而 $\left[\frac{y_1}{a_1}\right]-\left(-\left[\frac{x_1}{b_1}\right]\right)=\left[\frac{y_1}{a_1}\right]+\left[\frac{x_1}{b_1}\right]\geqslant\frac{y_1}{a_1}-\frac{a_1-1}{a_1}+\frac{x_1}{b_1}-\frac{b_1-1}{b_1}=\frac{a_1x_1+b_1y_1}{a_1b_1}-2+\frac{1}{a_1}+\frac{1}{b_1}=\frac{c_1}{a_1b_1}-2+\frac{1}{a_1}+\frac{1}{b_1}>\frac{a_1b_1-a_1-b_1}{a_1b_1}-2+\frac{1}{a_1}+\frac{1}{b_1}=-1$.

即有 $\left[\frac{y_1}{a_1}\right]\geqslant-\left[\frac{x_1}{b_1}\right]$，这说明使 $x\geqslant0,y\geqslant0$ 的 t 是存在的，那么方程 $a_1x+b_1y=c_1$ 有非负整数解，即①成立. 下面证明原题：

设 $a=a_0d,b=b_0d$，则 $(a_0,b_0)=1$，又知 $(c,d)=1$.

原方程变为 $d(a_0x+b_0y)+cz=n$,

$$d(a_0x+b_0y-(a_0b_0-a_0-b_0+1))+cz=n-a_0b_0d+a_0d+b_0d-d \qquad ②$$

设 $w=a_0x+b_0y-(a_0b_0-a_0-b_0+1)$，$n'=n-a_0b_0d+a_0d+b_0d-d$.

则②变为 $dw+cz=n'$，其中 $(d,c)=1$. 把它看成关于 w,z 的方程，由于 $n'=n-\frac{ab}{d}+a+b-d>\left(\frac{ab}{d}+cd-a-b-c\right)-\frac{ab}{d}+a+b-d=cd-c-d$，故由①的结论知 $dw+cz=n'$ 有非负整数解 w',z'.

于是 $a_0x+b_0y=w'+a_0b_0-a_0-b_0+1>a_0b_0-a_0-b_0$，而 $(a_0,b_0)=1$，再由①的结论知 $a_0x+b_0y=w'+a_0b_0-a_0-b_0+1$ 有非负整数解 x',y'. 由此我们得到 $x',y',z'\geqslant0$ 且满足 $ax'+by'+cz'=n$.

综上所述，原命题成立.

4. $$\begin{cases}x_n=\frac{1}{2}[(3+2\sqrt{2})^n+(3-2\sqrt{2})^n],\\y_n=\frac{1}{2\sqrt{2}}[(3+2\sqrt{2})^n-(3-2\sqrt{2})^n].\end{cases}$$

5. 证：只要对 x,y,z 是本原解来证明，不妨设 $2\mid y$，则存在一奇一偶的正整数 $r>s$，且 $(r,s)=1$，使得 $x=r^2-s^2,y=2rs,z=r^2+s^2$.

若 $3\nmid y$，则 $3\nmid r,3\nmid s$，因此必有 $r=3k\pm1,s=3h\pm1$.

不论何种情形均有 $3|x=r^2-s^2$，这就证明了(1).

若 $5\nmid y$，则 $5\nmid r, 5\nmid s$. 因此必有 $r=5k\pm1, 5k\pm2, s=5h\pm1, 5h\pm2$.

当 $r=5k\pm1, s=5h\pm1$ 或 $r=5k\pm2, s=5h\pm2$ 时必有 $5|x=r^2-s^2$.

当 $r=5k\pm1, s=5h\pm2$ 或 $r=5k\pm2, s=5h\pm1$ 时必有 $5|z=r^2+s^2$，(2)得证.

6. 提示：x,y,z 是勾股方程的本原解，进而利用定理 3，讨论 $x^2=a^2-b^2$ 或 $2ab$ 的解.

7. 解：设整数边直角三角形三边是 a,b,c，满足 $a^2+b^2=c^2$，其内切圆半径是 R，不妨设 $2|b$.

于是存在 $r,s\in\mathbf{N}_+, r>s, (r,s)=1$ 使得 $a=r^2-s^2, b=2rs, c=r^2+s^2$.

又 $(a+b+c)R=ab$，故 $R=\dfrac{ab}{a+b+c}=\dfrac{(r^2-s^2)\cdot 2rs}{2r^2+2rs}=\dfrac{(r+s)(r-s)rs}{r(r+s)}=s(r-s)\in\mathbf{Z}$.

从而命题成立.

8. 证：设 $kn+1$ 与 $(k+1)n+1$ 都是完全平方数，令 $kn+1=u^2, (k+1)n+1=v^2$

消去 n，得 $(k+1)u^2-kv^2=1$. ①

注意到，对①的任一正整数解 (u,v)，取 $n=u^2-v^2$，则容易得到 $kn+1$ 与 $(k+1)n+1$ 都是平方数，从而问题转化为证明①有无穷多个正整数解，作代换

$$\begin{cases}x=(k+1)u-kv,\\ y=v-u,\end{cases} \quad ②$$

则由①可得 $x^2-k(k+1)y^2=(k+1)u^2-kv^2=1$.

这是一个沛尔方程，它有无穷多组正整数解.

由②解得 $u=x+ky, v=x+(k+1)y$.

从而方程①也有无穷多组正整数解，命题得证.

9. 证：考虑沛尔方程 $x^2-2y^2=-1$ 它有无穷多组正整数解.

任取一组解 u,v，则 $2v^2=u^2+1$.

将上式两边同乘以 u^2 得 $2(uv)^2=(u^2+1)u^2$，故 $u^2<\sqrt{2}uv<u^2+1$.

所以 $[\sqrt{2}uv]=u^2$ 是一个平方数，即取 $n=uv$ 得出无穷多个符合要求的 n.

§4.2 同余分析法解不定方程

1. 证：用反证法

如果方程 $3y^2=(x^3+1)x$ 有一组整数解 x,y，由于 $(x,x^3+1)=1$，即存在 $u,v\in\mathbf{N}_+$，使得 $y=uv$，且 $3u^2=x^3+1, v^2=x$ 或 $u^2=x^3+1, 3v^2=x$.

前一种情况显然不可能，现假定后一种情况成立.

注意到，这时 $u^2=(x+1)(x^2-x+1)$，

由于 $x\equiv0\pmod{3}$，而 $x^2-x+1=(x+1)(x-2)+3$.

又 $x+1$ 与 x^2-x+1 互质，因此，存在正整数 t 满足 $x^2-x+1=t^2$.

容易看出，方程 $x^2-x+1=t^2$ 只有一个正整数解 $x=1$，但这与 $x\equiv0\pmod 3$ 矛盾. 因此，题目结论成立.

2. 证：若方程有整数解，则模 9 后有 $x^3+y^3+z^3\equiv4\pmod 9$.

但一完全立方数模 9 同余 0，1，−1 之一.

故 $x^3+y^3+z^3\equiv0,1,2,3,6,7,8\pmod 9$，矛盾. 故原命题成立.

3. 证：把原方程标为①式.

显然 $n>1$，此外，x 必是奇数，否则将①模 4 则产生矛盾. 进一步，n 也是奇数，因为若 $2|n$，则 x^n 为一个奇数的平方，从而①的右边 $\equiv1+2\equiv3\pmod 4$，但其左边 $\equiv1\pmod 4$，这不可能，故 $2\nmid n$.

设 $x+1=2^a x_1$，其中 x_1 为奇数，$a>0$（因 x 为奇数），将方程①改写为 $(x+2)^{2m}-1=x^n+1$. ②

②的左边有因子 $(x+2)^2-1=(2^a x_1+1)^2-1=2^{a+1}(2^{a-1}x_1^2+x_1)$，故 2^{a+1} 整除②的左边，但另一方面，由于 $n-1>0$ 为偶数，用二项式定理易得

$x^n+1=x(2^a x_1-1)^{n-1}+1\equiv x\cdot1+1\equiv2^a\cdot x_1\pmod{2^{a+1}}$，因 $2\nmid x_1$，故②的右边不能被 2^{a+1} 整除，矛盾. 所以原方程没有正整数解.

4. 解：模 4 即知方程 $12^m-5^n=-7$ 无正整数解，方程

$12^m-5^n=7$ ①

显然有解 $m=n=1$. 下面证明当 $m>1$ 时它无正整数解. 将①模 3 得 $-(-1)^n\equiv1\pmod 3$，故 n 为奇数，因此 $5^n\equiv5\pmod 8$. 又 $m\geqslant2$，故 $8|12^m$. 将①模 8 得出 $-5\equiv7\pmod 8$，这不可能，所以 $m=1$，从而 $n=1$.

5. 证：方程显然有解 $x=y=1$，将方程模 4 易知 y 为奇数，若 $y>1$，将方程模 9 得

$5^x\equiv2\pmod 9$ ①

不难求得对 $x=1,2,\cdots,5^x$ 模 9 周期为 5，7，8，4，2，1，故由①知 x 必有形式 $6k+5$，再将原方程模 7，易验证，对奇数 y，有 $3^y\equiv3,5,6\pmod 7$.

而 $x=6k+5$ 时，由费尔马小定理知 $5^6\equiv1\pmod 7$，故

$5^x=5^{6k+5}\equiv5^5\equiv3\pmod 7$.

从而原方程两边模 7 不等，因此它没有 $y>1$ 的解，故仅有的正整数解为 $y=1,x=1$.

6. 解：若正整数对 (a,b) 满足 $(ab^2+b+7)|(a^2b+a+b)$，则 $(ab^2+b+7)|[a(ab^2+b+7)-b(a^2b+a+b)]\Rightarrow(ab^2+b+7)|7a-b^2$.

(1) 当 $7a-b^2=0$ 时，得 $b=7k\,(k\in\mathbf{N}_+)$，代入得 $a=7k^2$.

此时有 $a^2b+a+b=k(ab^2+b+7)$，故 $(7k^2,7k)$ 是解.

(2) 当 $7a-b^2<0$ 时，有 $b^2-7a>0$，得 $b^2-7a\geqslant ab^2+b+7$，但这是不可能的.

(3) 当 $7a-b^2\geqslant0$ 时，有 $7a-b^2\geqslant ab^2+b+7$，得 $7a>ab^2\Rightarrow b=1$ 或 2.

若 $b=1$，则 $(a+8)\mid(a^2+a+1)$.

而 $a^2+a+1\equiv(-8)^2+(-8)+1(\bmod(a+8))$

$\equiv57(\bmod(a+8))$，

所以 $a+8=19$ 或 57，从而 $a=11$ 或 49.

此时又得两解 $\begin{cases}a=11,\\b=1;\end{cases}$ $\begin{cases}a=49,\\b=1.\end{cases}$

若 $b=2$，由 $ab^2+b+7\mid7a-b^2$ 得 $4a+9\mid7a-4$.

由于 $2(4a+9)>7a-4$，故只能是 $4a+9=7a-4$，但这不可能.

综合(1)，(2)，(3)知，所有解为 $(11,1)$，$(49,1)$，$(7k^2,7k)(k\in\mathbf{N}_+)$.

7. 解：设 $2^m+3^n=k^2(k\in\mathbf{N}_+)$. ①

①两边模 3，由于 $3\mid k$，则 $k^2\equiv1(\bmod3)$，故有 $(-1)^m\equiv1(\bmod3)$，得 $2\mid m$，$m\geqslant2$.

①两边模 4，由 k 是奇数知 $k^2\equiv1(\bmod4)$，故有 $(-1)^n\equiv1(\bmod4)$，得 $2\mid n$.

设 $m=2m_1$，$n=2n_1(m_1,n_1\in\mathbf{N}_+)$，有 $3^{2n_1}=k^2-2^{2m_1}=(k+2^{m_1})(k-2^{m_1})$.

由于 $(k+2^{m_1})-(k-2^{m_1})=2^{m_1+1}\not\equiv0(\bmod3)$，故 $k+2^{m_1}$，$k-2^{m_1}$ 中必有一个不是 3 的倍数，但它们均是 3 的幂，故只可能是 $k-2^{m_1}=1$，$k+2^{m_1}=2^{m_1+1}+1=3^{2n_1}$.

于是 $2^{m_1+1}=3^{2n_1}-1=(3^{n_1}+1)(3^{n_1}-1)$，又 $(3^{n_1}+1,3^{n_1}-1)=(3^{n_1}+1,2)=2$，所以必有 $3^{n_1}+1=2^{m_1}$，$3^{n_1}-1=2$，从而 $n_1=1$，$m_1=2\Rightarrow n=2$，$m=4$.

综上，所求 (m,n) 为 $(4,2)$.

8. 首先把原方程标为①，在①两边模 $x+1$ 得 $-(-1)^z\equiv1(\bmod x+1)$，

故 z 是奇数，将①分解为 $(x+1)^{y-1}=x^{z-1}-x^{z-2}+\cdots-x+1$，由此易知 x 是偶数，因为若 x 为奇数，则上式右边为奇数(z)个奇数之和，故是奇数，而左边是偶数，产生矛盾. 同样将①变形为

$(x+1)^{y-1}+(x+1)^{y-2}+\cdots+(x+1)+1=x^{z-1}$，可见 y 也是偶数.

现在设 $x=2x_1$，$y=2y_1$，则①可分解为

$((x+1)^{y_1}-1)((x+1)^{y_1}+1)=x^z$ ②

因 x 是偶数，故 $(x+1)^{y_1}-1$ 与 $(x+1)^{y_1}+1$ 的最大公约数是 2，又显然有 $x\mid(x+1)^{y_1}-1$，由这些及②推出必须 $(x+1)^{y_1}-1=2x_1^z$，$(x+1)^{y_1}+1=2^{z-1}$.

因此 $2^{z-1}>2x_1^z$，故 $x_1=1$，即 $x=2$，从而易得 $y=2$ 及 $z=3$.

9. 解：方程两边模 4 得

$x^3\equiv y^2+1(\bmod4)$，所以 $x^3\equiv1$ 或 $2(\bmod4)$.

若 x 为偶数，则 $x^3\equiv0(\bmod4)$，不成立，于是 x 为奇数.

方程化为 $y^2+1=(x+2)[(x-1)^2+3]$ ①

因 $2\mid x-1$，故 $(x-1)^2+3$ 是 $4k+3$ 型的数，其必含有 $4k+3$ 型的素因子 p，则在①两

边模 p 得

$y^2\equiv -1(\bmod p),(y^2)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}}(\bmod p)$,

即 $y^{p-1}\equiv -1(\bmod p)$（$\frac{p-1}{2}$是奇数）.

又由$(y,p)=1$,知上式与费尔马小定理矛盾.

从而原方程没有整数解.

10. 解：将方程改写为 $3^x-1=2^xy$ ①

这表明,如果(x,y)是解,则 x 不能超过 3^x-1 的标准分解中因子 2 的指数,记 $x=2^m(2n+1)$,其中 m,n 是非负整数,于是可得

$3^x-1=3^{2^m(2n+1)}-1=(3^{2n+1})^{2^m}-1=(3^{2n+1}-1)\prod\limits_{k=0}^{m-1}((3^{2n+1})^{2^k}+1)$ ②

由于 $3^{2n+1}=(1+2)^{2n+1}$

$\equiv 1+2(2n+1)+4n(2n+1)(\bmod 8)$（二项式定理）

$\equiv 3(\bmod 8)$,

则$(3^{2n+1})^{2^k}\equiv\begin{cases}3,当 k=0 时;\\1,当 k=1,2,\cdots 时\end{cases}(\bmod 8)$.

因此对于所求的指数,当 $m=0$ 时是 1,当 $m=1,2,\cdots$时是 $m+2$,由此可以断定,x 不能超过 $m+2$.

故 $2^m\leqslant 2^m(2n+1)=x\leqslant m+2$. 于是,$m\in\{0,1,2\}$且 $n=0$.

由此可断定,所给方程的正整数解是$(x,y)=(1,1),(2,2),(4,5)$.

11. 证：将方程两端相加,再同时加 1,可得

$(x^3+y+1)^2+z^9=147^{157}+157^{147}+1$. ①

下面证明,式①两边模 19 不同余.

选择模 19 是因为 2 和 9 的最小公倍数为 18,由费尔马小定理,当 a 不是 19 的倍数时,$a^{18}\equiv 1(\bmod 19)$.

特别地,$(z^9)^2\equiv 0$ 或 $1(\bmod 19)$,于是,有 $z^9\equiv -1,0,1(\bmod 19)$.

经计算可得 $n^2\equiv -8,-3,-2,0,1,4,5,6,7,9(\bmod 19)$,

由费尔马小定理有 $147^{157}+157^{147}+1\equiv 147^{13}+157^3+1(\bmod 19)$

$\equiv -5^{13}+5^3+1(\bmod 19)\equiv 14(\bmod 19)$.

因为 $z^9+n^2\not\equiv 14(\bmod 19)$,所以①式无整数解.

§4.3 各种方法的综合运用

1. 解：方程可分解为

$(x+y+z)(x+y-z)(-x+y+z)(x-y+z)=-2^3\times 3$ ①

由于 2 整除①的右边,故①的左边四个因数中至少有一个被 2 整除. 另一方面,这四

个数中任意两个的和显然是偶数，故它们的奇偶性相同，从而现在都是偶数，即①的左边被 2^4 整除，但①的右边不是 2^4 的倍数，因此方程无整数解.

2. 解：我们证明：若 $n>1,n\in\mathbf{N}_+$，则方程 $x(x+1)=y^n$ 无正整数解.

显然，$y\neq1$，设 p 是 y 的一个素因子，则 $p^n\mid x(x+1)$，又 $x=a^n,x+1=b^n$，a、b 是自然数，显然 $a<b$，若 $n>1$，$b^n-a^n=1$，则 $(b-a)(b^{n-1}+b^{n-2}a+\cdots+a^{n-1})=1$.

即 $b-a\geqslant1,b^{n-1}+b^{n-2}a+\cdots+a^{n-1}>1$，矛盾. 故结论成立.

于是原方程正无正整数解.

3. 解：设 $s=a+b+c,p(x)=(x-a)(x-b)(x-c)=x^3-sx^2+(ab+bc+ca)x-abc$.

则 $(a+b)(b+c)(c+a)=p(s)=(ab+bc+ca)s-abc$.

于是，题设等式可整理为 $(ab+bc+ca)s-abc=-2s^3+2-2abc$，

即 $p(-s)+2=0$.

这表明 $(2a+b+c)(a+2b+c)(a+b+2c)=2$.

易看出上式左边某个因子是 2，另外两个因子是 1，1（或 $-1,-1$），或者某个因子是 -2，另外两个因子是 $1,-1$（或 $-1,1$）.

当某个因子是 2 时，有 $\begin{cases}2a+b+c=2,\\a+2b+c=1,\\a+b+2c=1;\end{cases}$ 或 $\begin{cases}2a+b+c=2,\\a+2b+c=-1,\\a+b+2c=-1.\end{cases}$

分别解得 $a=1,b=0,c=0;a=2,b=-1,c=-1$.

当某个因子是 -2 时，相应的两个方程组可导出 $4(a+b+c)=-2$，显然该方程没有整数解 (a,b,c).

由于方程关于 a,b,c 是对称的，于是，(a,b,c) 的全部可能的值为 $(1,0,0),(0,1,0),(0,0,1),(2,-1,-1),(-1,2,-1),(-1,-1,2)$.

4. 解：显然 x 是奇数，记 t 中 2 的幂次为 $V_2(t)$.

若 m 是奇数，设 $y=x-1$，则 $x^m-1=(y+1)^m-1=y^m+C_m^1y^{m-1}+C_m^2y^{m-2}+\cdots+C_m^{m-1}y$.

其中 $C_m^{m-1}y$ 项中 2 的幂次为 y 中 2 的幂次，其余项均满足 $V_2(C_m^iy^i)=V_2(y)+(i-1)V_2(y)+V_2(C_m^i)>V_2(y)$，故 $V_2(x^m-1)=V_2(y)=V_2(x-1)$.

又 $V_2(x^m-1)=V_2(2^{2n+1}+2^n)=n$，有 $V_2(x-1)=n$.

则 $2^n\mid x-1$. 所以，$x-1\geqslant2^n,x\geqslant2^n+1$.

而 $x^3\geqslant(2^n+1)^3=2^{3n}+3\times2^{2n}+3\times2^n+1>2^{2n+1}+2^n+1=x^m$.

所以，$m<3$. 故 $m=1$，此时 $x=2^{2n+1}+2^n+1$.

若 m 为偶数，设 $m=2m_0$. 则 $(x^{m_0})^2=7\times2^{2n-2}+(2^{n-1}+1)^2$，

即 $(x^{m_0}-2^{n-1}-1)(x^{m_0}+2^{n-1}+1)=7\times2^{2n-2}$.

若 $n=1$，则 $x^m=2^3+2^1+1=8+2+1=11$ 不是平方数，不可能.

因此，$n\geqslant 2$.

所以，$x^{m_0}-2^{n-1}-1\not\equiv x^{m_0}+2^{n-1}+1 \pmod 4$.

又因为它们都是偶数，则它们之一中 2 的幂次为 1，只有下面四种情形：

$$\begin{cases}x^{m_0}-2^{n-1}-1=14,\\ x^{m_0}+2^{n-1}+1=2^{2n-3};\end{cases} \quad ①$$

$$\begin{cases}x^{m_0}-2^{n-1}-1=2^{2n-3},\\ x^{m_0}+2^{n-1}+1=14;\end{cases} \quad ②$$

$$\begin{cases}x^{m_0}-2^{n-1}-1=7\times 2^{2n-3},\\ x^{m_0}+2^{n-1}+1=2;\end{cases} \quad ③$$

$$\begin{cases}x^{m_0}-2^{n-1}-1=2,\\ x^{m_0}+2^{n-1}+1=7\times 2^{2n-3}.\end{cases} \quad ④$$

由①有 $2^{n-1}+1=2^{2n-4}-7$，即

$2^{n-4}+1=2^{2n-7}$，解得 $n=4$，$x^{m_0}=23$. 故 $x=23$，$m_0=1$.

由②有 $2^{n-1}+1=7-2^{2n-4}$，即 $2^{n-1}+2^{2n-4}=6$.

因为 $6=4+2$，故无解.

由③有 $2^{n-1}+1=1-7\times 2^{2n-4}$，也不可能.

由④有 $2^{n-1}+1=7\times 2^{2n-4}-1$，即 $2^{n-2}+1=7\times 2^{2n-5}$.

考察二进表中 1 的个数，故也不可能.

所以，$(x,m,n)=(2^{2n+1}+2^n+1,1,n)$，$(23,2,4)$.

5. 解： 注意到 $(a^3+b)(a+b^3)=(a+b)^4$

$\Leftrightarrow a^4+a^3b^3+ab+b^4=a^4+4a^3b+6a^2b^2+4ab^3+b^4$

$\Leftrightarrow a^3b^3+2a^2b^2+ab=4a^3b+8a^2b^2+4ab^3$

$\Leftrightarrow ab(ab+1)^2=4ab(a+b)^2$

$\Leftrightarrow ab[(ab+1)^2-4(a+b)^2]=0$

因此，$(a,0)$，$(0,b)$ 是给定方程的解，$a,b\in\mathbf{Z}$.

另外的解必须使得 $(ab+1)^2-4(a+b)^2=0$ 成立.

即 $ab+1=\pm 2(a+b)$ 成立.

如果 $ab+1=2(a+b)$，则有 $(a-2)(b-2)=3$.

于是，有 $\begin{cases}a-2=3\\ b-2=1\end{cases}$ 或 $\begin{cases}a-2=1\\ b-2=3\end{cases}$ 或 $\begin{cases}a-2=-3\\ b-2=-1\end{cases}$ 或 $\begin{cases}a-2=-1\\ b-2=-3\end{cases}$.

分别解得 $(a,b)=(5,3)(3,5)$，$(-1,1)$，$(1,-1)$.

如果 $ab+1=-2(a+b)$，则有 $(a+2)(b+2)=3$.

类似地解得$(a,b)=(1,-1),(-1,1),(-5,-3),(-3,-5)$.

综上所述，给定方程所有可能解的集合为$\{(a,0)\mid a\in\mathbf{Z}\}\cup\{(0,b)\mid b\in\mathbf{Z}\}\cup\{(-5,-3),(-3,-5),(-1,1),(1,-1),(3,5),(5,3)\}$.

6. 解：如果 p 是 $n+1$ 的质因子，则 p 也是 $n!+1$ 的质因子. 因为 $n!+1$ 不能被任何质数 $q(q\leqslant n)$ 整除，所以只能是 $p=n+1$.

如果 $n+1=2$，$n=1$ 且 $2^k-1=1$，则 $k=1$，因此，数对$(1,1)$是一个解.

如果 $n+1=3$，同理，得 $3^k-1=2$ 和 $k=1$，数对$(2,1)$是一个解.

如果 $n+1=5$，同理，得 $5^k-1=24$ 和 $k=2$. 因此，数对$(4,2)$是一个解.

假设(n,k)是满足条件的一个解，$n+1$ 是一个大于等于 7 的奇质数，那么，$n=2m$，$m>2$.

因为 $2\leqslant n-1$，$m\leqslant n-1$，$n=2m$ 是$(n-1)!$ 的因子，所以，$n!$ 能被 n^2 整除，因此

$(n+1)^k-1=n^k+kn^{k-1}+\cdots+\dfrac{k(k-1)}{2}n^2+nk$ 能被 n^2 整除.

于是，k 能被 n 整除，且 $k\geqslant n$，从而，

$n!=(n+1)^k-1>n^k\geqslant n^n>n!$，矛盾.

综上所述，所有的解为$(1,1),(2,1),(4,2)$.

7. 解：因为 $p^x=(y+1)(y^2-y+1)$，$y>0$，所以，$y+1\geqslant 2$.

令 $y+1=p^t(t\in\mathbf{N}_+,1\leqslant t\leqslant x)$，则 $y=p^t-1$.

从而，$y^2-y+1=p^{x-t}$.

将 $y=p^t-1$ 代入上式得$(p^t-1)^2-(p^t-1)+1=p^{x-t}$.

即 $p^{2t}-3p^t+3=p^{x-t}$.

故 $p^{x-t}(p^{3t-x}-1)=3(p^t-1)$.

(1)当 $p=2$ 时，$p^{3t-x}-1$，p^t-1 为奇数，则 p^{x-t} 为奇数.

故 $x=t$，$y^2-y+1=1$，因此，$y=1$，$p=2$，$x=1$.

(2)当 $p\neq 2$ 时，p 为奇数，则 $p^{3t-x}-1$，p^t-1 为偶数，p^{x-t} 为奇数.

从而，$3\mid p^{x-t}$ 或 $3\mid(p^{3t-x}-1)$.

当 $3\mid p^{x-t}$ 时，$p=3$，$x=t+1$，则 $y^2-y+1=3$，得 $y=2$，$x=3$.

当 $3\mid(p^{3t-x}-1)$时，有 $p^{x-t}\mid(p^t-1)\Rightarrow x=t$.

同(1)得 $y=1$，$p=2$，矛盾.

综上所述，有两组解 $p=2,x=1,y=1$ 和 $p=3,x=2,y=2$.

8. 解：原方程化为

$(x+y+z)[(x-y)^2+(y-z)^2+(z-x)^2]=4006=2\times 2003$，

且$(x-y)^2+(y-z)^2+(z-x)^2\equiv 0(\bmod 2)$，

所以，$\begin{cases}x+y+z=1,\\(x-y)^2+(y-z)^2+(z-x)^2=4006;\end{cases}$ ①

或 $\begin{cases}x+y+z=2003,\\(x-y)^2+(y-z)^2+(z-x)^2=2.\end{cases}$ ②

对于①有 $(x-y)^2+(x+2y-1)^2+(2x+y-1)^2=4006$，

即 $6x^2+6y^2+6xy-6x-6y+2=4006$.

但 $4006\equiv4(\bmod 6)$，矛盾.

对于②，因为 $|x-y|,|y-z|,|z-x|$ 中有两个 1，一个 0，不妨设 $x\geqslant y\geqslant z$.

当 $x-1=y=z$ 时，$3y+1=2003$，无解.

当 $x=y=z+1$ 时，$3x-1=2003$，$x=668$.

因此，满足条件的三元整数组为 $(668,668,667)$，$(668,667,668)$，$(667,668,668)$.

9. 解：如果 $b<0$，则对所有 $|a|>1$，数 a^b 不是整数.

对于 $a=1$，可得 $1=b+2$，$b=-1$.

对于 $a=-1$，可得 $(-1)^b=-b+2$，此方程无解，事实上，由 $b<0$，有 $-b+2\geqslant3$，但 $(-1)^b=\pm1$.

当 $b=0$ 时，所给的方程无解.

当 $b>0$ 时，数 a^b 能被 a 整除，于是 a 整除 2，这是因为 $a^b-ab=2$，因此，$a=-2,-1,1,2$.

若 $a=-2$，有 $(-2)^b=-2b+2$，即 $(-2)^{b-1}=b-1$ 不可能有 $b\in\mathbf{Z}$ 满足这个方程.

事实上，如果数 b 满足方程，它应该是奇数，即 $b=2s+1$. 方程可改写为 $4^s=2s$. 这不可能，因为对任何实数 s，都有 $4^s>2s$.

若 $a=-1$，则有 $(-1)^b=-b+2$，即 $|-b+2|=1$.

因此 $b=1$ 或 3，但只有 $b=3$ 满足方程 $(-1)^b=-b+2$.

若 $a=1$，则有 $1=b+2$，在条件 $b>0$ 的情况下无解.

若 $a=2$，则有 $2^b=2(b+1)$，即 $2^{b-1}=b+1$，只有一个解 $b=3$.

当 $b>3$ 时，易用数学归纳法证明 $2^{b-1}>b+1$.

因此，满足方程的全部数对 (a,b) 为 $(2,3)$，$(1,-1)$，$(-1,3)$.

10. 解：假设 (x,y,n) 为满足

$$\frac{x!+y!}{n!}=3^n \quad ①$$

的自然数三元组，易知 $n\geqslant1$.

假设 $x\leqslant y$，考虑下面两种情况：

(1) $x\leqslant n$，易知 $\frac{x!+y!}{n!}=3^n\Leftrightarrow1+\frac{y!}{x!}=3^n\cdot\frac{n!}{x!}$ ②

由式②可推出 $1+\frac{y!}{x!}\equiv 0 \pmod 3$.

因为 3 个连续整数的乘积能被 3 整除，又因为 $n\geqslant 1$，则有 $x<y\leqslant x+2$.

（ⅰ）如果 $y=x+2$，由式②得 $1+(x+1)(x+2)=3^n\cdot\frac{n!}{x!}$ ③

因 $2\mid(x+1)(x+2)$，由式③知 $n\leqslant x+1$.

若 $n=x$，则式③化为 $1+(x+1)(x+2)=3^x$，

即 $x^2+3x+3=3^x$. ④

因为 $x\geqslant 1$，由式④知 $x\equiv 0 \pmod 3$，所以，$x\geqslant 3$，同时得到 $-3=x^2+3x-3^x\equiv 0 \pmod 9$，矛盾. 因此，$n\neq x$，故 $n=x+1$.

于是，式③化为 $1+(x+1)(x+2)=3^n(x+1)$，

所以，$x+1$ 是 1 的正因子，即 $x=0$. 因此，$x=0,y=2,n=1$.

（ⅱ）如果 $y=x+1$，由式②得 $x+2=3^n\cdot\frac{n!}{x!}$. ⑤

因为 $n\geqslant 1$，由式⑤知 $x\geqslant 1$，则 $x=n$ 且 $x+2=3^x$. ⑥

易知 $x=1$ 是满足式⑥的唯一自然数.

在这两种情况中，如果三元数组 (x,y,n) 满足式①，则 $(x,y,n)=(0,2,1)$ 或 $(1,2,1)$.

(2) $x>n$，易知 $\frac{x!+y!}{n!}=3^n\Leftrightarrow\frac{x!}{n!}\left(1+\frac{y!}{x!}\right)=3^n$. ⑦

因为 $n+1$ 和 $n+2$ 不能同时为 3 的幂，由式⑦可推出 $x=n+1$.

于是，式⑦化为 $n+1+\frac{y!}{n!}=3^n$. ⑧

因为 $y\geqslant x$，则 $y\geqslant n+1$.

令 $A=\frac{y!}{(n+1)!}$，代入式⑧得 $(n+1)(A+1)=3^n$. ⑨

如果 $y\geqslant n+4$，则 $A\equiv 0 \pmod 3$，故 $A+1$ 不能为 3 的幂.

于是，由式⑨得 $y\leqslant n+3$，所以 $n+1\leqslant y\leqslant n+3$.

（ⅰ）若 $y=n+3$，则 $A=(n+2)(n+3)$，

由式⑨得 $(n+1)[1+(n+2)(n+3)]=3^n$，即 $(n+2)^3-1=3^n$ ⑩

由此可得 $n>2$，$n+2\equiv 1 \pmod 3$.

令 $n+2=3k+1$，$k\geqslant 2$，由式⑩有

$9k(3k^2+3k+1)=3^{3k-1}$ 与 $(3k^2+3k+1,3)=1$ 矛盾，有 $y\neq n+3$.

（ⅱ）若 $y=n+2$，则 $A=n+2$.

由式⑨得 $(n+1)(n+3)=3^n$.

当 $n\geqslant 1$ 时，$(n+1)$ 和 $(n+3)$ 不能同时为 3 的幂，所以 $y\neq n+2$.

(ⅲ)若 $y=n+1$,则 $A=1$.由⑨得 $2(n+1)=3^n$.

显然不存在满足上式的 n,所以 $y\neq n+1$.

综上所述,满足式①的三元数组为 $(x,y,n)=(0,2,1)$ 或 $(2,0,1)$ 或 $(1,2,1)$ 或 $(2,1,1)$.

经检验,这四组解满足条件.

第五章　高斯函数

§5.1　高斯函数的定义与基本性质

1. A　设 $a=[x]=[y]$,则 $a\leqslant x,y<a+1$,自然有 $|x-y|<1$,反之,取 $x=-\frac{1}{3}$,$y=\frac{1}{3}$,则 $|x-y|<1$,但 $[x]\neq[y]$.

2. D　$(\sqrt{3}+\sqrt{2})^{2006}=(5+2\sqrt{6})^{1003}$.设 $f(n)=(5+2\sqrt{6})^n+(5-2\sqrt{6})^n(n\in\mathbf{N})$,则 $f(n+2)=10f(n+1)-f(n)\equiv-f(n)\pmod{10}$.故 $f(n+4)\equiv-f(n+2)\equiv f(n)\pmod{10}$.所以 $f(n)$ 是以 4 为周期的模周期函数,模为 10.于是 $f(1003)\equiv f(3)=-f(1)\equiv-10\equiv0\pmod{10}$.

3. A　对于 $0\leqslant x\leqslant100$,令 $x=3n+r$,其中 n 为非负整数,r 为实数且 $0\leqslant r<3$.于是

$f(x)=[3n+r]+[6n+2r]+\left[5n+\frac{5r}{3}\right]+[9n+3r]+[12n+4r]=35n+f(r)$.

所以对每个 $n\geqslant0$,在区间 $[n,n+3)$ 上函数 f 给出的不同整数值的个数相同.

由于 $f(x)$ 是阶梯函数,且它的值至少在点 $[x]$,$[2x]$,$\left[\frac{5x}{3}\right]$,$[3x]$,$[4x]$ 之一跳跃.而函数 $f(x)$ 在 $[0,3)$ 上有以下 22 次跳跃:$0,\frac{1}{4},\frac{1}{3},\frac{1}{2},\frac{3}{5},\frac{2}{3},\frac{3}{4},1,\frac{6}{5},\frac{5}{4},\frac{4}{3},\frac{3}{2},\frac{5}{3},\frac{7}{4},\frac{9}{5},2,\frac{9}{4},\frac{7}{3},\frac{12}{5},\frac{5}{2},\frac{8}{3},\frac{11}{4}$.从而 $f(x)$ 在区间 $[0,3)$ 上所取的不同值的个数为 22,在 $[0,99)$ 上取不同值的个数为 $33\times22=726$,又因为 $f(x)$ 在 $[99,100]$ 上所取不同值的个数与 $f(x)$ 在 $[0,1]$ 上所取的不同值个数相同,在 $[0,1]$ 上 $f(x)$ 有 8 次跳跃,故 $f(x)$ 在 $[99,100]$ 上所取的不同的值的个数为 8 个.

综上可知 f 在 $[0,100]$ 上所取不同的整数值的个数为 $726+8=734$.

4. A　设 $n=x_1+x_2+\cdots+x_{A(n)}$;$x_1<x_2<\cdots<x_{A(n)}$ 均为正整数,则有 $x_1\geqslant1$,$x_2\geqslant2$,$\cdots$,$x_{A(n)}\geqslant A(n)$,因此 $n\geqslant1+2+\cdots+A(n)=\frac{1}{2}A(n)(A(n)+1)$,从而正整数 $A(n)\leqslant\left[\frac{\sqrt{8n+1}-1}{2}\right]$.

又 $n=1+2+\cdots+\left(\left[\frac{\sqrt{8n+1}-1}{2}\right]-1\right)+\left(\left[\frac{\sqrt{8n+1}-1}{2}\right]+x\right)$，其中 x 为整数且由 $n\geqslant 1+2+\cdots+A(n)$ 知 $x\geqslant 0$. 所以 $A(n)\geqslant\left[\frac{\sqrt{8n+1}-1}{2}\right]$. 综上所述，$A(n)=\left[\frac{\sqrt{8n+1}-1}{2}\right]$.

5. D 当 $i=1$ 时，$\frac{1}{[\sqrt[4]{(i+2)(i+3)}]}-\frac{1}{[\sqrt[4]{i(i+5)}]}=\frac{1}{\sqrt[4]{12}}-\frac{1}{\sqrt[4]{6}}=\frac{1}{1}-\frac{1}{1}=0$；

当 $i=2$ 时，$\frac{1}{[\sqrt[4]{(i+2)(i+3)}]}-\frac{1}{[\sqrt[4]{i(i+5)}]}=\frac{1}{\sqrt[4]{20}}-\frac{1}{\sqrt[4]{10}}=\frac{1}{2}-\frac{1}{1}=-\frac{1}{2}$；

当 $i=3$ 或 $i=4$ 时，$\frac{1}{[\sqrt[4]{(i+2)(i+3)}]}-\frac{1}{[\sqrt[4]{i(i+5)}]}=\frac{1}{2}-\frac{1}{2}=0$；

当 $i\geqslant 5$ 时，$(i+2)^2<i(i+5)<(i+2)(i+3)<(i+3)^2$，此时 $\sqrt{i+2}<\sqrt[4]{i(i+5)}<\sqrt[4]{(i+2)(i+3)}<\sqrt{i+3}$. 假设此时 $[\sqrt[4]{i(i+5)}]\neq[\sqrt[4]{(i+2)(i+3)}]$，则存在 $n\in\mathbf{N}_+$ 使得 $\sqrt[4]{i(i+5)}<n\leqslant\sqrt[4]{(i+2)(i+3)}$. 于是 $\sqrt{i+2}<n<\sqrt{i+3}$，即 $i+2<n^2<i+3$，亦即 $n^2-3<i<n^2-2$. 但区间 (n^2-3,n^2-2) 内无整数，与 $i\in\mathbf{N}_+$ 相矛盾. 这样我们就证明了当 $i\geqslant 5$ 时必有 $\frac{1}{[\sqrt[4]{(i+2)(i+3)}]}=\frac{1}{[\sqrt[4]{i(i+5)}]}$.

综上所述，原式 $=0+\left(-\frac{1}{2}\right)+0\times 2+0\times 2002=-\frac{1}{2}$.

6. C 由 $a_1=1,a_2=2,a_{n+2}=a_n+a_{n+1},n\in\mathbf{N}_+$ 易知对任意 $n\in\mathbf{N}_+$ 均有 $a_n\in\mathbf{N}_+$，且 $a_1<a_2<\cdots<a_n<\cdots$. 从而 $a_{n+2}=a_n+a_{n+1}<a_{n+1}+a_{n+1}=2a_{n+1}$，即 $\frac{a_{n+2}}{a_{n+1}}<2$，所以 $1<\frac{a_{n+2}}{a_{n+1}}<2$. 于是 $\left\{\frac{a_{n+2}}{a_{n+1}}\right\}=\frac{a_{n+2}}{a_{n+1}}-1=\frac{a_{n+1}+a_n}{a_{n+1}}-1=\frac{a_n}{a_{n+1}}$，$n\in\mathbf{N}_+$. 所以原式 $=\left[\frac{a_2}{a_1}\right]\cdot\left[\frac{a_{98}}{a_2}\right]\cdot\frac{a_1}{a_2}\cdot\frac{a_2}{a_3}\cdot\cdots\cdot\frac{a_{97}}{a_{98}}=\left[\frac{a_2}{a_1}\right]\cdot\left[\frac{a_{98}}{a_2}\right]\cdot\frac{a_1}{a_{98}}=2\cdot\left[\frac{a_{98}}{2}\right]\cdot\frac{1}{a_{98}}$. 而由递推式 $a_{n+2}=a_n+a_{n+1}$ 及 $a_1=1$，$a_2=2$ 易通过数学归纳法知 a_{3k+2} 为偶数，a_{3k+1} 与 a_{3k+3} 为奇数 $(k\in\mathbf{N})$，所以 a_{98} 为偶数，原式 $=2\cdot\frac{a_{98}}{2}\cdot\frac{1}{a_{98}}=1$.

7. 1 设 $n^2=\left[\frac{n^2}{A}\right]A+r,0\leqslant r<A$，显然 $A\neq n$，因为若 $A=n$. 就由 $n\left|\left[\frac{n^2}{A}\right]+1\right.$ 得 $n\left|\left[\frac{n^2}{n}\right]+1=n+1\right.$，$n=1$，但 $n>1$，矛盾！

故需分 $0<A<n$ 与 $n<A<n^2$ 两种情况讨论.

由 $n^2=\left[\frac{n^2}{A}\right]A+r$ 得 $n^2=\left(\left[\frac{n^2}{A}\right]+1\right)A-(A-r)$ ①

(1)当 $0<A<n$ 时，由①及 $n\left|\left[\frac{n^2}{A}\right]+1\right.$ 知 $n\mid A-r$. 而 $0<A-r<n$. 所以不存在满足条件的 A.

(2)当 $n<A<n^2$ 时，有 $\left[\frac{n^2}{A}\right]<\frac{n^2}{A}<n$. 则 $\left[\frac{n^2}{A}\right]+1<n+1$，又由 $n\left|\left[\frac{n^2}{A}\right]+1\right.$ 可设 $\left[\frac{n^2}{A}\right]+1=nB$，于是 $nB<n+1$，此时只可能有 $B=1$，这时 $\left[\frac{n^2}{A}\right]+1=n$. 代入①有 $n^2=nA-(A-r)$，则 $A=\frac{n^2-r}{n-1}=n+1-\frac{r-1}{n-1}$.

若 $1\neq r<n$，则 $r-1\geqslant n-1$，A 不为整数，若 $r\geqslant n$，则 $\frac{r-1}{n-1}\leqslant 1$，结合 $A=n+1-\frac{r-1}{n-1}$ 即得 $A\leqslant n$，与 $A>n$ 相矛盾，所以只有 $r=1$，即 $A=n+1$.

综上可知存在唯一的 $A=n+1$ 满足要求.

8. $\frac{1927}{22}$　由 $44^2=1936<2006<2025=45^2$ 知对任意 $k\in\{1,2,\cdots,2006\}$，存在某个 $n\in\{1,2,\cdots,44\}$ 使得 $n^2\leqslant k<(n+1)^2$. 此时 $\frac{1}{[\sqrt{k}]}=\frac{1}{n}$.

$$\text{故}\sum_{k=1}^{2006}\frac{1}{[\sqrt{k}]}=\sum_{1\leqslant k<2^2}\frac{1}{[\sqrt{k}]}+\sum_{2^2\leqslant k<3^2}\frac{1}{[\sqrt{k}]}+\cdots+\sum_{43^2\leqslant k<44^2}\frac{1}{[\sqrt{k}]}$$

$$+\sum_{44^2\leqslant k\leqslant 2006}\frac{1}{[\sqrt{k}]}=\sum_{1\leqslant k<2^2}\frac{1}{1}+\sum_{2^2\leqslant k<3^2}\frac{1}{2}+\cdots+\sum_{43^2\leqslant k<44^2}\frac{1}{43}+\sum_{44^2\leqslant k\leqslant 2006}\frac{1}{44}$$

$$=\frac{2^2-1}{1}+\frac{3^2-2^2}{2}+\cdots+\frac{44^2-43^2}{43}+\frac{2006-44^2+1}{44}=\frac{3}{1}+\frac{5}{2}+\cdots+\frac{87}{43}+\frac{71}{44}$$

$$=2\times 43+\frac{71}{44}+\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{43}.$$

故原式 $=86+\frac{71}{44}+\sum_{k=1}^{43}\frac{1}{k}-\sum_{k=1}^{44}\frac{1}{k}=86+\frac{70}{44}=\frac{1927}{22}$.

9. 76304　首先，若 $\{x\}+\{y\}=1$，则 $[x+y]=[x]+[y]+1$，$x,y\in\mathbf{R}$，事实上，$[x]+[y]+1=x-\{x\}+y-\{y\}+1=x+y+1-(\{x\}+\{y\})=x+y$，而由 $[x]+[y]+1=x+y$ 这个式子可看出 $x+y\in\mathbf{Z}$，故 $x+y=[x+y]$，所以 $[x+y]=x+y=[x]+[y]+1$.

503 是一个质数，因此，对于 $n=1,2,\cdots,502$，$\frac{502n}{503}\notin\mathbf{Z}$.

但是 $\frac{305n}{503}+\frac{305(503-n)}{503}=305$，故 $\left\{\frac{305n}{503}\right\}+\left\{\frac{305(503-n)}{503}\right\}=1$.

于是$\left[\frac{305n}{503}+\frac{305(503-n)}{503}\right]=\left[\frac{305n}{503}\right]+\left[\frac{305(503-n)}{503}\right]+1$.

所以$\left[\frac{305n}{503}\right]+\left[\frac{305(503-n)}{503}\right]=304$.

$S=\sum_{n=1}^{502}\left[\frac{305n}{503}\right]=\sum_{n=1}^{251}\left(\left[\frac{305n}{503}\right]+\left[\frac{305(503-n)}{503}\right]\right)=304\times 251=76304$.

10. 600　令 $f(x)=[2x]+[4x]+[6x]+[8x]$.

当 x 在 $(0,1]$ 中变化时，$f(x)$ 的值在 12 个跳跃点：$\frac{1}{8},\frac{1}{6},\frac{1}{4},\frac{1}{3},\frac{3}{8},\frac{1}{2},\frac{5}{8},\frac{2}{3},\frac{3}{4},\frac{5}{6},\frac{7}{8},1$ 处改变，所以 $f(x)$ 在 1～20 中取 12 个不同的正整数值. 另一方面 $f(x+n)=f(x)+20n$ 对任意正整数 n 成立，将 1～1000 分为 50 段，每 20 个为 1 段，每段中，$f(x)$ 可取 12 个值，故总共可取 $50\times 12=600$ 个值，亦即在前 1000 个正整数中有 600 个可表示成 $[2x]+[4x]+[6x]+[8x]$ 的形式.

11. $\left\{\frac{1}{2}\right\}\cup\left[\frac{5}{6},\frac{5}{4}\right)$　由对称性不妨设 $x\geqslant 1$.

(1) 当 $x=1$ 时，$f(x)=\frac{1}{2}$；

(2) 当 $x>1$ 时，令 $x=n+\alpha$，其中 $n\in\mathbf{N}_+$，$0\leqslant\alpha<1$. 则 $\frac{1}{x}=\frac{1}{n+\alpha}$，$\left[\frac{1}{x}\right]=0$，$[x]=n$.

$$f(x)=\frac{n+\alpha+\frac{1}{n+\alpha}}{n+1} \qquad ①$$

注意到函数 $y=x+\frac{1}{x}$ 在 $x>1$ 时为增函数.

考虑函数①，由于 $n\leqslant n+\alpha<n+1$，则 $\frac{n+\frac{1}{n}}{n+1}\leqslant f(x)<\frac{n+1+\frac{1}{n+1}}{n+1}$.

记 $a_n=\frac{n+\frac{1}{n}}{n+1}$，$b_n=\frac{n+1+\frac{1}{n+1}}{n+1}$，

则 $a_n-a_{n+1}=\frac{n^2+1}{n(n+1)}-\frac{(n+1)^2+1}{(n+1)(n+2)}=\frac{2-n}{n(n+1)(n+2)}$，

于是当 $n\geqslant 1$ 时，有 $a_1>a_2$，$a_2=a_3$，$a_3<a_4<a_5<\cdots$，即 $a_2=a_3$ 最小. $b_n-b_{n+1}=\frac{(n+1)^2+1}{(n+1)^2}-\frac{(n+2)^2+1}{(n+2)^2}=\frac{2n+3}{(n+1)^2(n+2)^2}>0$.

于是当 $n\geqslant 1$ 时，有 $b_1>b_2>b_3>b_4>\cdots$，即 b_1 最大.

所以当 $x>1$ 时，$f(x)$ 的值域为 $[a_2,b_1)=\left[\frac{5}{6},\frac{5}{4}\right)$.

于是 $f(x)$ 的值域为 $\left\{\frac{1}{2}\right\}\cup\left[\frac{5}{6},\frac{5}{4}\right)$.

12. 251　设方程 $x^3-3x^2+1=0$ 的三根依次为 α,β,a，则由 $f(-1)<0$，$f\left(-\frac{1}{2}\right)>0$，$f\left(\frac{1}{2}\right)>0$，$f(1)<0$，$f(2\sqrt{2})<0$，$f(3)>0$（这里 $f(x)=x^3-3x^2+1$）知可设 $-1<\alpha<-\frac{1}{2}$，$\frac{1}{2}<\beta<1$，$2\sqrt{2}<a<3$，由于 $f(-\alpha)=-2\alpha^3+(\alpha^3-2\alpha^2+1)=-2\alpha^3>0$，于是 $-\alpha<\beta$，$|\alpha|<\beta$.

另一方面，由韦达定理知 $\alpha^2+\beta^2=(\alpha+\beta)^2-2\alpha\beta=(3-a)^2+\frac{2}{a}=9+\frac{2-6a^2+a^3}{a}=9+\frac{-2a^3+a^3}{a}=1+(8-a^2)$. 又因为 $a^2>(2\sqrt{2})^2=8$，故 $\alpha^2+\beta^2<1$.

定义 $\mu_n=\alpha^n+\beta^n+a^n(n=0,1,2,\cdots)$，则 $\mu_0=3$，$\mu_1=2+\beta+a=3$，$\mu_2=\alpha^2+\beta^2+a^2=9$，$\mu_{n+3}=3\mu_{n+2}-\mu_n(n\geqslant 0)$.

又因为 $0<\alpha^2+\beta^2<1$，故 $a^n=\mu_n-(\alpha^n+\beta^n)=\mu_n-1-[1-(\alpha^n+\beta^n)]$. 所以 $[a^n]=\mu_n-1$.（$n=1,2,\cdots$），故 $17\mid[a^n]\Leftrightarrow 17\mid\mu_n-1$.

现在考察 $\{\mu_n\}$ 在模 17 意义下的情况：$\mu_0\equiv 3$，$\mu_1\equiv 3$，$\mu_2\equiv 9$，$\mu_3\equiv 7$，$\mu_4\equiv 1$，$\mu_5\equiv 11$，$\mu_6\equiv 9$，$\mu_7\equiv 9$，$\mu_8\equiv 16$，$\mu_9\equiv 5$，$\mu_{10}\equiv 6$，$\mu_{11}\equiv 2$，$\mu_{12}\equiv 1$，$\mu_{13}\equiv 14$，$\mu_{14}\equiv 6$，$\mu_{15}\equiv 0$，$\mu_{16}\equiv 3$，$\mu_{17}\equiv 3$，$\mu_{18}\equiv 9$，…可见在模 17 下，$\{\mu_n\}$ 是 16 为周期的模周期数列，即 $\mu_{n+16}\equiv\mu_n\pmod{17}$，故可知 $17\mid[a^n]\Leftrightarrow n\equiv 4$ 或 $12\pmod{16}$. 而在 $1\leqslant n\leqslant 2006$ 时，有 $\left[\frac{2006}{16}\right]\times 2+1=251$ 个 n 满足 $n\equiv 4$ 或 $12\pmod{16}$.

13. 证：设 $m\in\mathbf{N}_+$，m 为奇数，并记 $(\sqrt{2}+1)^m=x_m\sqrt{2}+y_m$，其中 $x_m,y_m\in\mathbf{N}$.

由二项式定理知 $(\sqrt{2}-1)^m=x_m\sqrt{2}-y_m$.

将上述二式相乘得 $2x_m^2-y_m^2=1$.

从而 $2x_m^2=y_m^2+1$，$y_m^2<2x_m^2$.

于是有 $y_m^4<2x_m^2y_m^2=y_m^2(y_m^2+1)<(y_m^2+1)^2$.

因此 $y_m^2<\sqrt{2}x_my_m<y_m^2+1$，故 $[\sqrt{2}x_my_m]=y_m^2$.

令 $n=x_my_m$，则 $a_n=[\sqrt{2}x_my_m]=y_m^2$. 显然，这样的 a_n 有无穷多个，命题得证.

14. 证：令 $k=\left[\sqrt{\frac{n}{3}}+\frac{1}{2}\right]$，则

$$f(n)=\left[n+\sqrt{\frac{n}{3}}+\frac{1}{2}\right]=n+\left[\sqrt{\frac{n}{3}}+\frac{1}{2}\right]=n+k.$$

正整数 k 满足 $k\leqslant\sqrt{\frac{n}{3}}+\frac{1}{2}<k+1$.

于是 $k+2>\sqrt{\frac{n}{3}}+1+\frac{1}{2}>\sqrt{\frac{n+1}{3}}+\frac{1}{2}\geqslant k$.

$$f(n+1)=\left[n+1+\sqrt{\frac{n+1}{3}}+\frac{1}{2}\right]=n+1+\left[\sqrt{\frac{n+1}{3}}+\frac{1}{2}\right]$$

$$=\begin{cases}n+k+1, 若\sqrt{\frac{n+1}{3}}+\frac{1}{2}<k+1,\\ n+k+2, 若\sqrt{\frac{n+1}{3}}+\frac{1}{2}\geqslant k+1.\end{cases}$$

若 $\sqrt{\frac{n+1}{3}}+\frac{1}{2}<k+1$,则 $f(n)$ 随 n 的增加逐次增加 1;

若 $\sqrt{\frac{n+1}{3}}+\frac{1}{2}\geqslant k+1$,则 $f(n)$ 跳过一个自然数 $n+k+1$.

由于 $\sqrt{\frac{n+1}{3}}+\frac{1}{2}\geqslant k+1\geqslant\sqrt{\frac{n}{3}}+\frac{1}{2}$

$\Leftrightarrow n+1\geqslant 3\left(k+\frac{1}{2}\right)^2>n$

$\Leftrightarrow n+1\geqslant 3k^2+3k+\frac{3}{4}>n\Leftrightarrow n=3k^2+3k$.

所以 $f(n)$ 跳过的数为 $n+k+1=3k^2+3k+k+1=3(k+1)^2-2(k+1)=a_{k+1}$.

又因为 $f(1)=2$. 故 $f(n)$ 历遍除数列 $a_n=3n^2-2n$ 的项之外的所有正整数.

15. 首先证明一个等式:

对一切实数 x,有 $\left[x+\frac{1}{2}\right]=[2x]-[x]$, ①

设 $x=[x]+\alpha$,则 $0\leqslant\alpha<1$,于是有

$\left[x+\frac{1}{2}\right]=\left[[x]+\alpha+\frac{1}{2}\right]=[x]+\left[\alpha+\frac{1}{2}\right]$, ②

$[2x]-[x]=[2[x]+2\alpha]-[[x]+\alpha]=[x]+[2\alpha]-[\alpha]$, ③

由②与③知①式 $\Leftrightarrow\left[\alpha+\frac{1}{2}\right]=[2\alpha]-[\alpha]$, $0\leqslant\alpha<1$.

当 $0\leqslant\alpha<\frac{1}{2}$ 时,$\frac{1}{2}\leqslant\alpha+\frac{1}{2}<1$, $0\leqslant 2\alpha<1$,于是

$\left[\alpha+\frac{1}{2}\right]=0$，$[2\alpha]-[\alpha]=0$，等式$\left[\alpha+\frac{1}{2}\right]=[2\alpha]-[\alpha]$成立.

当$\frac{1}{2}\leqslant\alpha<1$时，$1\leqslant\alpha+\frac{1}{2}<\frac{3}{2}$，$1\leqslant 2\alpha<2$，于是

$\left[\alpha+\frac{1}{2}\right]=1$，$[2\alpha]-[\alpha]=1$，等式$\left[\alpha+\frac{1}{2}\right]=[2\alpha]-[\alpha]$也成立.

因此①式成立，由①可得

$$\left[\frac{n+2^k}{2^{k+1}}\right]=\left[\frac{n}{2^{k+1}}+\frac{1}{2}\right]=\left[2\cdot\frac{n}{2^{k+1}}\right]-\left[\frac{n}{2^{k+1}}\right]=\left[\frac{n}{2^k}\right]-\left[\frac{n}{2^{k+1}}\right],$$

于是有

$$\sum_{k=0}^{\infty}\left[\frac{n+2^k}{2^{k+1}}\right]=\left([n]-\left[\frac{n}{2}\right]\right)+\left(\left[\frac{n}{2}\right]-\left[\frac{n}{2^2}\right]\right)+\left(\left[\frac{n}{2^2}\right]-\left[\frac{n}{2^3}\right]\right)+\cdots$$

而当$k\to\infty$时，对固定的$n<2^k$有$\left[\frac{n}{2^k}\right]=0$.

从而知$\sum_{k=0}^{\infty}\left[\frac{n+2^k}{2^{k+1}}\right]=[n]=n$.

§5.2 高斯方程与不等式

1. D　显然$x>0$，由对称性不妨设$x\geqslant 1$，则由$x\neq 1$得$x>1$，于是$\left[\frac{1}{x}\right]=0$，$[x]+\left[\frac{1}{x}\right]=3$，此时$3\leqslant x<4$. 而当$0<x<1$时，$\frac{1}{4}<x\leqslant\frac{1}{3}$，故$3\leqslant x<4$，$\frac{1}{4}<x\leqslant\frac{1}{3}$为原方程的解.

2. B　设$[x]=a$，$\{x\}=b$，则由$x^2-[x^2]=\{x\}^2$得$(a+b)^2-[(a+b)^2]=b^2$，

即$(a+b)^2-a^2-[b^2+2ab]=b^2$. 故$2ab=[b^2+2ab]$.

由此可知$2ab\in\mathbf{Z}$，而当$2ab\in\mathbf{Z}$时，由$0\leqslant b<1$知$0\leqslant b^2<1$，故此时$2ab=[b^2+2ab]$，这意味着x是方程的解$\Leftrightarrow 2ab\in\mathbf{Z}$. 对任意$a\in\{1,2,\cdots,m-1\}$，都有$a$个$b$满足要求，加上$x=m$，便有$m(m-1)+1$个解.

3. C　由于$\frac{19}{100},\frac{20}{100},\cdots,\frac{91}{100}$均小于1，故等式左边每一项为$[r]$或$[r]+1$，而左边共73项，$73\times 7<546<73\times 8$，故$[r]=7$. 设$\left[r+\frac{k}{100}\right]=7(19\leqslant k\leqslant m)$，$\left[r+\frac{p}{100}\right]=8(m+1\leqslant p\leqslant 91)$，则$7(m-18)+8(91-m)=546$，得$m=56$，故$\left[r+\frac{56}{100}\right]=7$，即$6.44\leqslant r<7.44$；$\left[r+\frac{57}{100}\right]=8$，即$7.43\leqslant r<8.43$，故$7.43\leqslant r<7.44$. 所以$[100r]=743$.

4. B　设$[3x+1]=t$，则t为整数且$0\leqslant(3x+1)-t<1$.　①

于是原方程即为 $t=2x-\frac{1}{2}$，亦即 $x=\frac{1}{2}t+\frac{1}{4}$.

将上式代入①中可得 $0\leqslant\frac{3}{2}t+\frac{3}{4}+1-t<1$.

即 $-\frac{7}{2}\leqslant t\leqslant-\frac{3}{2}$ ②

由②及 $t\in\mathbf{Z}$ 知 $t=-2$ 或 $t=-3$.

当 $t=-2$ 时，$x_1=-\frac{3}{4}$；当 $t=-3$ 时，$x_2=-\frac{5}{4}$.

所以 $x_1+x_2=\left(-\frac{3}{4}\right)+\left(-\frac{5}{4}\right)=-2$.

5. B　由于 $\left[\frac{10^n}{x}\right]=2006$，于是，$2006\leqslant\frac{10^n}{x}<2007$，故 $\frac{10^n}{2006}<x\leqslant\frac{10^n}{2007}$，即 $0.00049850\cdots<x<0.00049825\cdots$ 所以 $n\geqslant7$ 时，$\left(\frac{10^n}{2006},\frac{10^n}{2007}\right]$ 内含有整数，所以 n 的最小值为 7.

6. D　设 $m=\left[\frac{n^2}{5}\right]$.

(1)当 $n=5k(k\in\mathbf{N}_+)$ 时，$m=\left[\frac{25k^2}{5}\right]=5k^2$，仅当 $k=1$ 时，m 为素数，此时 $n=5$.

(2)当 $n=5k+1(k\in\mathbf{N})$ 时，$m=\left[\frac{(5k+1)^2}{5}\right]=5k^2+2k=k(5k+2)$，仅当 $k=1$ 时，m 为素数，此时 $n=6$.

(3)当 $n=5k+2(k\in\mathbf{N})$ 时，$m=\left[\frac{(5k+2)^2}{5}\right]=5k^2+4k=k(5k+4)$.

当 $k=1$ 时，$m=9$ 为合数，因此对所有 $k\in\mathbf{N}_+$，m 均为合数.

(4)$n=5k+3(k\in\mathbf{N})$ 时，$m=\left[\frac{(5k+3)^2}{5}\right]=(5k+1)(k+1)$.

当 $k=0$ 时，$m=1$，当 $k\in\mathbf{N}_+$ 时 m 为合数.

(5)$n=5k+4(k\in\mathbf{N})$ 时，$m=\left[\frac{(5k+4)^2}{5}\right]=(5k+3)(k+1)$.

当 $k=0$ 时，$m=3$ 为素数，当 k 为正整数时，m 为合数，此时 $n=4$.

所以 $n=4,5,6$ 时 $\left[\frac{n^2}{5}\right]$ 为素数，这样 n 的倒数和为 $\frac{37}{60}$.

7. $x=\sqrt[3]{\frac{4}{3}}$　(1)若 $x\leqslant-1$，则 $3x^3-[x]\leqslant3x-x+1<0$；(2)若 $-1\leqslant x<0$，则 $3x^3-[x]=3x^3+1\leqslant1$；(3)若 $x\geqslant2$，则 $3x^3-[x]\geqslant3x^3-x>3x-x\geqslant4$；(4)若 $0\leqslant x<1$，则 $3x^3-[x]=3x^3<3$；(5)若 $1\leqslant x<2$，则 $3x^3-[x]=3x^3-1=3$，$x=\sqrt[3]{\frac{4}{3}}$. 由此知方程只有一

个解 $x=\sqrt[3]{\frac{4}{3}}$.

8. $x=1+2\sqrt{7}$ 或 $x=1+2\sqrt{10}$.

设 $\frac{x-1}{2}=y$，则 $x^2-2x-3=(x-1)^2-4=4y^2-4$，即 $4y^2-4=12[y]$，亦即 $y^2-1=3[y]$. 故 $y^2-1=3[y]\leqslant 3y$，且 $y^2-1=3[y]>3(y-1)$. 由 $y^2-1\leqslant 3y$ 得 $\frac{3-\sqrt{13}}{2}\leqslant y\leqslant\frac{3+\sqrt{13}}{2}$，由 $y^2-1>3(y-1)$ 得 $y>2$ 或 $y<1$，所以 $\frac{3-\sqrt{13}}{2}\leqslant y<1$ 或 $2<y\leqslant\frac{3+\sqrt{13}}{2}$. 所以 $[y]=-1$，或 0，或 2，或 3.

若 $[y]=-1$，则由 $y^2-1=3[y]$ 得 $y^2=-2$，矛盾！若 $[y]=0$，则由 $y^2-1=3[y]$ 得 $y=\pm1$，矛盾！若 $[y]=2$，则 $y=\sqrt{7}$，若 $[y]=3$，则 $y=\sqrt{10}$，综上，$y=\sqrt{7}$ 或 $\sqrt{10}$.

所以 $x=1+2\sqrt{7}$ 或 $x=1+2\sqrt{10}$.

9. $x=1,\sqrt{33},\sqrt{41},7$

设 $[x]=n$，则已知方程可写为 $x^2+7=8n$，因此 $n>0$.

由 $n\leqslant x<n+1$ 得 $n^2+7\leqslant x^2+7<(n+1)^2+7=n^2+2n+8$.

且 $n^2+7\leqslant 8n<n^2+2n+8$. 所以 $n^2-8n+7\leqslant 0$，且 $n^2-6n+8>0$.

解得 $1\leqslant n<2$ 或 $4<n\leqslant 7$，故 $n=1,5,6,7$. 则有 $x^2+7=8,40,48,56$ 解得 $x=\pm1,\pm\sqrt{33},\pm\sqrt{41},\pm7$.

因为 $n\geqslant 0$，所以 $x\geqslant 0$，故只有 $x=1,\sqrt{33},\sqrt{41},7$.

10. $\left[1+\frac{1}{n},1+\frac{1}{n-1}\right)$

由题设，x 必为整数，当 $x<0$ 时，$[ax]<ax<x$，所以 $x\geqslant 0$，令 $\{a\}=a-[a]$，则原方程为 $x=[ax]=[a]x+[\{a\}x]$，由于 $[a]\geqslant 1$，故上式成立 $\Leftrightarrow [a]=1$，且 $\{a\}x<1$，又因为 $x=0$ 显然满足要求.

所以 $x<\frac{1}{\{a\}}$ 恰对 $n-1$ 个正整数 $1,2,\cdots,n-1$ 成立，从而 $\frac{1}{n}\leqslant\{a\}<\frac{1}{n-1}$. 即 $1+\frac{1}{n}\leqslant a<1+\frac{1}{n-1}$.

11. $\{x\mid x=k\pi+\frac{\pi}{4},k\in\mathbf{Z}\}$

令 $\tan x=y$，则由 $2\cos^2x=\cos 2x+1=\frac{1-\tan^2x}{1+\tan^2x}$，知 $[y]=\frac{1-y^2}{1+y^2}+1=\frac{2}{1+y^2}>0$，故 $[y]\geqslant 1$，于是 $y\geqslant 1$，由 $y\geqslant 1$ 知 $\frac{2}{1+y^2}\leqslant\frac{2}{1+1^2}=1$，所以 $1\leqslant[y]\leqslant 1$ 即 $[y]=1$，从而 $y=1$，

即 $\tan x=1$.

12. $\varnothing$　$[\log_2 1]+[\log_2 2]+\cdots+[\log_2 128]+\cdots+[\log_2 2^{55}]=2\times1+4\times2+8\times3+16\times4+32\times5+64\times6+128\times7=1538$，于是$[\log_2 256]+[\log_2 257]+\cdots+[\log_2 n]=2006-1538=468<256\times8$，而 $8\nmid 468$，故不存在满足条件的 n.

13. 解：令$[x]=n$，$\{x\}=\alpha$，则 $x=n+\alpha$，$\alpha\in[0,1)$，则原方程即为 $4x^2-40x+51=-40\alpha$，因为 $\alpha\in[0,1)$，所以$-40<4x^2-40x+51\leqslant0$. 解得$\frac{3}{2}\leqslant x<\frac{7}{2}$或$\frac{13}{2}<x\leqslant\frac{17}{2}$.

(1)$\frac{3}{2}\leqslant x<2$ 时，$n=1$，$4x^2-40+51=0$，无实数解；

(2)$2\leqslant x<3$ 时，$[x]=2$，$4x^2-80+51=0$，$x=\frac{\sqrt{29}}{2}$（舍去了$-\frac{\sqrt{29}}{2}$）；

(3)$3\leqslant x<\frac{7}{2}$时，$n=3$，$4x^2-120+51=0$，$x=\pm\frac{\sqrt{69}}{2}$舍去；

(4)$\frac{13}{2}\leqslant x<7$ 时，$n=6$，$4x^2-240+51=0$，$x=\frac{\sqrt{189}}{2}$（舍去了$-\frac{\sqrt{189}}{2}$）；

(5)$7\leqslant x<8$ 时，$n=7$，$4x^2-280+51=0$，$x=\frac{\sqrt{229}}{2}$（舍去了$-\frac{\sqrt{229}}{2}$）；

(6)$8\leqslant x<\frac{17}{2}$时，$n=8$，$4x^2-320+51=0$，$x=\frac{\sqrt{269}}{2}$（舍去了$-\frac{\sqrt{269}}{2}$）.

故原方程的解有 4 个：$x_1=\frac{\sqrt{29}}{2}$，$x_2=\frac{\sqrt{189}}{2}$，$x_3=\frac{\sqrt{229}}{2}$，$x_4=\frac{\sqrt{269}}{2}$.

14. 解：题中条件$\Leftrightarrow$对一切 $n\in\mathbf{N}_+$ 均有 $k^2+\frac{n}{k^2}\geqslant2006$　　①

且存在 $k\in\mathbf{N}_+$ 使得 $k^2+\frac{n}{k^2}<2007$　　②

①$\Leftrightarrow$对一切 $k\in\mathbf{N}_+$ 有 $k^4-2006k^2+n\geqslant0$，

即$(k^2-1003)^2+n-1003^2\geqslant0$　　③

因为$[\sqrt{1003}]=31$，而 $31^2-1003=-42$，$32^2-1003=21$.

故③式左边在 k 取 32 时最小，因此①$\Leftrightarrow n\geqslant2006\times32^2-32^4=1024\times982$.

又因为②$\Leftrightarrow$存在 $k\in\mathbf{N}_+$ 使$\left(k^2-\frac{2007}{2}\right)^2+n-\left(\frac{2007}{2}\right)^2<0$，

上式左边也在 $k=32$ 时最小，故②$\Leftrightarrow n<2007\times32^2-32^4=1024\times983$.

故 n 为满足 $1024\times982\leqslant n\leqslant1024\times982+1023$ 的一切整数.

15. 解：根据对称性不妨设 $a\leqslant b$.

由 $x-1<[x]\leqslant x$ 知$\frac{b^2}{a}+\frac{a^2}{b}-2<\left[\frac{a^2}{b}\right]+\left[\frac{b^2}{a}\right]\leqslant\frac{a^2}{b}+\frac{b^2}{a}$，及 $ab+\frac{a^2+b^2}{ab}-1<$

$\left[\frac{a^2+b^2}{ab}\right]+ab\leqslant\frac{a^2+b^2}{ab}+ab.$

即 $-1<\frac{a^2}{b}+\frac{b^2}{a}-\frac{a^2+b^2}{ab}-ab<2$，$-ab<a^3+b^3-a^2-b^2-a^2b^2<2ab$.

所以 $b^3-(a^2+1)b^2-2ab+a^3-a^2<0$ ①

$b^3-(a^2+1)b^2+ab+a^3-a^2>0$ ②

在①中，若 $b\geqslant a^2+2$，则 $b^3-(a^2+1)b^2-2ab+a^3-a^2$

$=b[b(b-a^2-1)-2a]+a^3-a^2\geqslant b(b-2a)+a^3-a^2$

$=(b-a)^2+a^3-2a^2\geqslant(a^2-a+2)^2+a^3-2a^2$

$=(a^2-a+2)^2-a^2+a^2(a-1)=(a^2+2)(a^2-2a+2)+a^2(a-1)>0$，与①矛盾.

故 $b\leqslant a^2+1$.

在②中，设 $f(x)=x^3-(a^2+1)x^2+ax+a^3-a^2$.

当 $a\geqslant2$ 时，有 $f(-a)=-a^3-(a^2+1)a^2-a^2+a^3-a^2<0$，

又因为 $f(0)=a^3-a^2>0$ 且 $f(a)=a^2(-a^2+2a-1)<0$.

而 $f(a^2)=a^2(-a^2+2a-1)<0$，$f(a^2+1)=a(2a^2-a+1)>0$.

因此方程 $f(x)=0$ 的三个根在区间 $(-a,0)$，$(0,a)$，(a^2,a^2+1) 中各有一个.

故当 $a\leqslant b\leqslant a^2$ 时，$f(b)<0$ 与②相矛盾，所以 $b\geqslant a^2+1$.

当 $a=1$ 时，②即为 $b^3-2b^2+b>0\Leftrightarrow b(b-1)^2>0$，所以 $b\geqslant2=a^2+1$.

总之无论 a 为多少均有 $b\geqslant a^2+1$.

由 $b\leqslant a^2+1$ 及 $b\geqslant a^2+1$ 知 $b=a^2+1$.

将 $b=a^2+1$ 代入原式得

$$\left[\frac{a^2}{a^2+1}\right]+\left[\frac{a^4+2a^2+1}{a}\right]=\left[\frac{a^2+1}{a}+\frac{1}{a^2+1}\right]+a(a^2+1).$$

当 $a\geqslant2$ 时，上式即为 $a^3+2a=a+a(a^2+1)$，是恒等式.

当 $a=1$ 时，上式即为 $\left[\frac{1}{2}\right]+\left[\frac{1+2+1}{1}\right]=\left[\frac{2}{1}+\frac{1}{2}\right]+(1+1)$，显然成立.

因此 $a\leqslant b$ 时，原方程的解为 $b=a^2+1$，$a\in\mathbf{N}$.

故原方程的所有解为 $b=a^2+1$，$a\in\mathbf{N}$，或 $a=b^2+1$，$b\in\mathbf{N}$.

§5.3 高斯函数的应用

1. 解：设 $x=10p+q$，p、q 为整数且 $0\leqslant q\leqslant9$.

则 $\left[\frac{x}{10}\right]=\left[p+\frac{q}{10}\right]=p$.

从而 $\left[\frac{x-1}{10}\right]=\left[p+\frac{q-1}{10}\right]$ 的值为 $p-1$（$q=0$ 时）或 p（$q\neq0$ 时），$x-10\left[\frac{x-1}{10}\right]$ 的值为 10（$q=0$ 时）或 q（$q\neq0$ 时），

$\left[\lg\dfrac{10}{x-10\left[\dfrac{x-1}{10}\right]}\right]$的值为 1($q=1$ 时)或 0($q\neq1$ 时).

于是 $f(x)=f(p)+1(q=1$ 时)或 $f(p)(q\neq1$ 时).

故可知 $f(x)$的值即为 x 的十进制表示中数字 1 的个数，所以当 $0\leqslant x\leqslant2006$ 时，$f(x)$的最大值为 4，此时 $x=1111$.

2. 解：所求最大正数 $c=\dfrac{\sqrt{2}}{4}$.

若 $c>0$，则对 $n\in\mathbf{N}$ 有 $\{n\sqrt{2}\}\geqslant\dfrac{c}{n}$.

取 $n_k=\dfrac{(\sqrt{2}+1)^{4k+1}+(\sqrt{2}-1)^{4k+1}}{2\sqrt{2}}$，则 $n_k\in\mathbf{N}_+$，且

$$\begin{aligned}\sqrt{2}n_k&=\frac{1}{2}((\sqrt{2}+1)^{4k+1}+(\sqrt{2}-1)^{4k+1})\\&=\frac{1}{2}((\sqrt{2}+1)^{4k+1}-(\sqrt{2}-1)^{4k+1})+(\sqrt{2}-1)^{4k+1}.\end{aligned}$$

由于 $0<(\sqrt{2}-1)^{4k+1}<1$，所以

$$[\sqrt{2}n_k]=\frac{1}{2}((\sqrt{2}+1)^{4k+1}-(\sqrt{2}-1)^{4k+1}),\{\sqrt{2}n_k\}=(\sqrt{2}-1)^{4k+1}.$$

$$n_k\{\sqrt{2}n_k\}=\frac{[(\sqrt{2}+1)^{4k+1}+(\sqrt{2}-1)^{4k+1}](\sqrt{2}-1)^{4k+1}}{2\sqrt{2}}=\frac{1+(\sqrt{2}-1)^{2(4k+1)}}{2\sqrt{2}}.$$

故当 $k\to+\infty$ 时有 $n_k\{\sqrt{2}n_k\}\to\dfrac{1}{2\sqrt{2}}$.

于是 $c\leqslant\dfrac{1}{2\sqrt{2}}$.

另一方面，设 $m=[n\sqrt{2}]$，则 $n\sqrt{2}>m>n\sqrt{2}-1$.

从而 $1\leqslant2n^2-m^2=n^2\left(\sqrt{2}+\dfrac{m}{n}\right)\left(\sqrt{2}-\dfrac{m}{n}\right)<n^2\left(\sqrt{2}-\dfrac{m}{n}\right)>2\sqrt{2}$.

于是对一切 $n\in\mathbf{N}$，

$$\frac{1}{2\sqrt{2}n}<n\left(\sqrt{2}-\frac{m}{n}\right)=n\sqrt{2}-m=\{n\sqrt{2}\}.$$

综上可知 $c_{\max}=\dfrac{\sqrt{2}}{4}$.

3. 证：设 p 是不大于 n 的任意一个素数.

则 p 在 $n!$ 中的幂指数为

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots<\frac{n}{2}+\frac{n}{2^2}+\cdots=\frac{\frac{1}{2}n}{1-\frac{1}{2}}=n,$$

如果 $p|b$,则 p 在分子中的次数$\geqslant n-1$,而分母中 p 的次数$\leqslant n-1$,于是分母中的素因子 p 可完全约去.

如果 $p\nmid b$,则 p 必能整除 $a,a+b,\cdots,a+(p-1)b$ 中的一个,因此 n 个数 $a,a+b,\cdots,a+(n-1)b$ 中至少有$\left[\frac{n}{p}\right]$个数能被 p 整除,同样,至少有$\left[\frac{n}{p^2}\right]$个数能被 p^2 整除,等等.

所以 p 在乘积 $a(a+b)\cdots[a+(n-1)b]$ 中次数 k 应满足 $k\geqslant\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots$

因此分母中 $n!$ 的素因数 p 可被完全约去.

综上可知$\frac{b^{n-1}a(a+b)(a+2b)\cdots[a+(n-1)b]}{n!}$为整数.

4. 证:令 $m=2^\alpha-1$,则 $m!$ 中含因子 2 的个数为$\left[\frac{2^\alpha-1}{2}\right]+\left[\frac{2^\alpha-1}{2^2}\right]+\cdots+\left[\frac{2^\alpha-1}{2^\alpha}\right]$

$=(2^{\alpha-1}-1)+(2^{\alpha-2}-1)+\cdots+(1-1)$

$=(2^{\alpha-1}+2^{\alpha-2}+\cdots+1)-\alpha=2^\alpha-1-\alpha.$

即 $n(m)=2^\alpha-1-\alpha.$

取 $\alpha=3^{2006}$,则 $m=2^\alpha-1=(2^\alpha-1-\alpha)+\alpha=3^{2006}+n(m)$,

故下面只需证明 $m>2006^{2006}$.

事实上,$m=2^{3^{2006}}-1>2^{3^{2005}}=2^{3^{2002}\cdot 3^3}=(2^{27})^{3^{2002}}>2006^{3^{2002}}>2006^{2006}$.

故命题得证.

5. 解:首先证明数列$\{a_n\}$单调递增且它具有如下形式:$m+\frac{k}{m}$,$0\leqslant k\leqslant m-1$.

当 $n=1$ 时,结论显然成立.

假定 $a_n=m+\frac{k}{m}$,$0\leqslant k\leqslant m-1$,则$[a_n]=\left[m+\frac{k}{m}\right]=m$.

于是 $a_{n+1}=a_n+\frac{1}{[a_n]}=\left(m+\frac{k}{m}\right)+\frac{1}{m}=m+\frac{k+1}{m}$.

从而 $a_{n+1}=\begin{cases}m+1,\text{当 } k=m-1 \text{ 时};\\ m+\frac{l}{m},l\leqslant m-1,\text{当 } k<m-1 \text{ 时}.\end{cases}$

因此数列有 1 项的整数部分为 1,有 2 项的整数部分为 2,…,于是整数部分不超过 19 的项有

$$1+2+3+\cdots+19=\frac{19\times 20}{2}=190.$$

而 $a_{191}=20$，故当 $n>191$ 时，$a_n>20$.

6. 证：令 $c(n)=\sqrt{4n+1}$，并设 $k(n)$ 是使得 $k+\frac{n}{k}$ 最小的 k 值.

则 $b(n-1)\leqslant k(n)+\frac{n-1}{k(n)}<k(n)+\frac{n}{k(n)}=b(n)$.

即有 $b(n-1)<b(n)$， ①

由 $k+\frac{m^2}{k}\geqslant 2\sqrt{k\times\frac{m^2}{k}}=2m(m\in\mathbf{N})$ 知当 $k=m$ 时，$k+\frac{m^2}{k}$ 取得最小值 $2m$，即对正整数 m 有 $b(m^2)=2m$. ②

又对正整数 m，当且仅当 $k=m$ 或 $k=m+1$ 时，$k+\frac{m^2+m}{k}$ 取得最小值 $2m+1$，即 $b(m^2+m)=2m+1$ ③

由①，②，③得 $[b(n)]=2m$，当 $m^2\leqslant n<m^2+m$；$[b(n)]=2m+1$，当 $m^2+m\leqslant n<(m+1)^2$. 另一方面，$c(n)=\sqrt{4n+1}$ 也是一个增函数，且

$c(m^2-1)=\sqrt{4m^2-3}<2m$，$c(m^2)=\sqrt{4m^2+1}>2m$，

$c(m^2+m)=\sqrt{4m^2+4m+1}=2m+1$.

由此知 $[c(n)]=2m$，当 $m^2\leqslant n<m^2+m$；$[c(n)]=2m+1$，当 $m^2+m\leqslant n<(m+1)^2$.

故 $[b(n)]=[c(n)]=[\sqrt{4n+1}]$.

7. 解：注意到 $|A|=r-1$，$|B|=s-1$，$|M|=n-2$，且 $r+s=n$. 故 A 与 B 构成 M 的一个划分 $\Leftrightarrow A\cap B=\varnothing$.

必要性：若 r 与 s 中的某个与 n 有公因数 d，则由 $n=r+s$ 可知 d 也是 r 与 s 的公因数，设 $r=r'\cdot d$，$s=s'\cdot d$，于是 $\left[\frac{r'\cdot n}{r}\right]=\left[\frac{s'\cdot n}{s}\right]$，故 $A\cap B=\varnothing$.

充分性：假设 $A\cap B\neq\varnothing$，即存在整数 a 与 b 使得 $\left[\frac{an}{r}\right]=\left[\frac{bn}{s}\right]=p$，其中 $1\leqslant a\leqslant r-1$，$1\leqslant b\leqslant s-1$，$p$ 为整数. 由于 r 和 s 均与 n 互素，则 $\frac{in}{r}$ 与 $\frac{in}{s}$ 均不为整数（$1\leqslant i\leqslant r-1$，$1\leqslant j\leqslant s-1$），于是 $p<\frac{an}{r}<p+1$，$p<\frac{bn}{s}<p+1$.

相加得 $p<a+b<p+1$，即两个整数之和介于两个整数之间，矛盾！故充分性得证.

8. 证：对任何 $k\in\{1,2,\cdots,n-1\}$，记 $mk=n\left[\frac{mk}{n}\right]+r_k$，其中 $r_k\in\{1,2,\cdots,n-1\}$，可得出以下几个结论：

(1) 由 $(m,n)=1$ 知 r_k 互不相同，所以 $\{r_1,r_2,\cdots,r_{n-1}\}=\{1,2,\cdots,n-1\}$.

(2) $\left\{\frac{mk}{n}\right\}=\frac{r_k}{n}(k=1,2,\cdots,n-1)$；

(3) 由 $2\mid m$，$2\nmid n$ 知 $\left[\frac{mk}{n}\right]\equiv r_k\pmod 2$，

故 $(-1)^{\left[\frac{mk}{n}\right]}=(-1)^{r_k}(k=1,2,\cdots,n-1)$．

由上述结论知 $s=\frac{1}{n}\sum\limits_{k=1}^{n-1}(-1)^{r_k}r_k=\frac{1}{n}\sum\limits_{k=1}^{n-1}(-1)^k k=\frac{1}{2}-\frac{1}{2n}$．

第六章　无穷递降法

§6.1　用无穷递降法解不定方程

1. 解：假设方程有非零整数解 (x_1,y_1,u_1,v_1)，则 $x_1^2+y_1^2=3(u_1^2+v_1^2)$．显然 $3\mid(x_1^2+y_1^2)$，若 $3\nmid x_1$ 或 $3\nmid y_1$，则 $x_1^2+y_1^2\equiv1,2\pmod 3$，这种情形是不成立的，所以必有 $3\mid x_1$，$3\mid y_1$，设 $x_2=\frac{x_1}{3}$，$y_2=\frac{y_1}{3}$，则 $(3x_2)^2+(3y_2)^2=3(u_1^2+v_1^2)$，即 $u_1^2+v_1^2=3(x_2^2+y_2^2)$，即 (u_1,v_1,x_2,y_2) 也是原方程的一组解，但此时有 $u_1^2+v_1^2+x_2^2+y_2^2<x_1^2+y_1^2+u_1^2+v_1^2$，反复进行如上的变形，所得解的平方和都严格地减少（由这些都为整数知至少减小 1），这显然是不可能的，所以，原方程没有非零整数解．

2. 解：$x_0=y_0=z_0$ 是方程的解，设方程另有解 (x,y,z)，若 x,y,z 中有三个或两个奇数，则 $x^2+y^2+z^2\equiv2$ 或 $3\pmod 4$，而 $x^2y^2\equiv0$ 或 $1\pmod 4$，这显然不可能；若 x,y,z 中恰有 1 个奇数，则 x,y 中至少有一个偶数，于是 $x^2y^2\equiv0\pmod 4$，但 $x^2+y^2+z^2\equiv1\pmod 4$，矛盾，因此，$x,y,z$ 必都为偶数．

设 $x_1=\frac{x}{2}$，$y_1=\frac{y}{2}$，$z_1=\frac{z}{2}$（x_1,y_1,z_1 为整数），则有 $(2x_1)^2+(2y_1)^2+(2z_1)^2=(4x_1y_1)^2$，即 $x_1^2+y_1^2+z_1^2=4x_1^2y_1^2$，该方程右端能被 4 整除，则 x_1,y_1,z_1 必均为偶数（否则 $x_1^2+y_1^2+z_1^2\equiv1$ 或 2 或 $3\pmod 4$，矛盾），于是可设 $x_2=\frac{x_1}{2}$，$y_2=\frac{y_1}{2}$，$z_2=\frac{z_1}{2}$，则 x_2,y_2,z_2 均为整数且 $(2x_2)^2+(2y_2)^2+(2z_2)^2=4\cdot(4x_1y_1)^2$，即 $x_2^2+y_2^2+z_2^2=16x_2^2y_2^2$．

继续如上的讨论，我们可得 3 个无穷整数列 $\{x_n\}$，$\{y_n\}$，$\{z_n\}$，其中 $z_k=\frac{1}{2}z_{k-1}$，$x_k=\frac{1}{2}x_{k-1}$，$y_k=\frac{1}{2}y_{k-1}(k\geqslant2)$，$x_1=\frac{1}{2}x$，$y_1=\frac{1}{2}y$，$z_1=\frac{1}{2}z$，但是任何非零整数都不能被 2 的所有方幂整除，所以 x,y,z 全为 0，这与假设矛盾，所以原方程只有 $x_0=y_0=z_0=0$ 这唯一一组整数解．

3. 解：设 (a,b,c,d) 是原方程的一组不全为零的一组整数解，显然 $6\mid d$，令 $d_1=\frac{d}{6}$，代

入原方程可得 $6a^2+3b^2+c^2=30d_1^2$，知 $3|c$，设 $c_1=\frac{c}{3}$，则可得 $2a^2+b^2+3c_1^2=10d_1^2$，于是只要证明方程 $2x^2+y^2+3z^2=10w^2$ 没有使 $w>0$ 的整数解，否则必有一组解 (x,y,z,w)，使 w 取最小正值，由于 y^2+3z^2 为偶数，故 y 与 z 同奇偶，若 y 与 z 同为奇数，则 $y^2\equiv z^2\equiv 1(\mathrm{mod}8)$，$10w^2\equiv 0$ 或 $2(\mathrm{mod}8)$，而 $2x^2+y^2+3z^2\equiv 4$ 或 $6(\mathrm{mod}8)$ 不可能等于 $10w^2$，因此 y 与 z 必同为偶数，设 $z_1=\frac{z}{2}$，$y_1=\frac{y}{2}$，则有 $x^2+2y_1^2+6z_1^2=5w^2$，此时 x 与 w 必同奇偶，如果 x 与 w 同为奇数，则 $x^2\equiv 1(\mathrm{mod}8)$，$2y_1^2\equiv 0$ 或 $2(\mathrm{mod}8)$，$6z_1^2\equiv 0$ 或 $6(\mathrm{mod}8)$，$5w^2\equiv 5(\mathrm{mod}8)$，故 $x^2+2y_1^2+6z_1^2\equiv 1$ 或 3 或 $7(\mathrm{mod}8)$，不可能有 $5w^2=x^2+2y_1^2+6z_1^2$，于是 x 与 w 同为偶数，设 $x_1=\frac{x}{2}$，$w_1=\frac{w}{2}$，则有 $2x_1^2+y_1^2+3z_1^2=2w_1^2$，由于 $0<w_1<w$，这与 w 的定义矛盾，进而知原方程只有解 $a=b=c=d=0$。

4. 证明：若 $a=b$，则 $k=\frac{2a^2}{a^2-1}=2+\frac{2}{a^2-1}$.

则 $(a^2-1)|2$ 且 $a^2-1>0$.

所以 $a^2-1=1$ 或 2，但这与 $a\in\mathbf{N}_+$ 矛盾.

所以 $a\neq b$，不妨 $a>b$.

当 $b=1$ 时，$k=\frac{a^2+1}{a-1}=a+1+\frac{2}{a-1}$，则 $(a-1)|2$ 且 $a\geqslant b+1=2$，所以 $a=2$ 或 3，无论哪种情形，都有 $k=5$.

不妨设 (a,b) 是使 $\frac{a^2+b^2}{ab-1}=k$ 的所有有序二元数组中使 $a+b$ 达到最小值的一组.

由 $\frac{a^2+b^2}{ab-1}=k$，得 $a^2-kb\cdot a+b^2+k=0$ ①

视①式为关于 a 的一元二次方程，则由韦达定理知该方程两根为 a，$(kb-a)$ 且 $kb-a=\frac{b^2+k}{a}>0$，又 $kb-a\in\mathbf{Z}$，所以 $kb-a\in\mathbf{N}_+$，且 $\frac{(kb-a)^2+b^2}{(kb-a)b-1}=k$，则由 (a,b) 的定义知

$a+b\leqslant\frac{b^2+k}{a}+b\left(\frac{b^2+k}{a}=kb-a\right)$，所以 $a^2-b^2\leqslant k=\frac{a^2+b^2}{ab-1}$.

于是 $a^2-b^2<\frac{a^2+b^2}{ab-1}+2<\frac{(a+b)^2}{ab-1}$. 所以 $\frac{a+b}{ab-1}>a-b\geqslant 1$. 即 $(a-1)(b-1)<2$.

显然 $b\leqslant 2$，若 $b=1$，由前面的结论知 $k=5$. 若 $b=2$，则 $a-1<2$ 且 $a>b=2$，矛盾.

综上可知 $k=5$.

5. 证明：原方程组为

$$\begin{cases}y^2+z^2=t^2 & ①\\ z^2-y^2=x^2 & ②\end{cases}$$

假设存在正整数 x,y,z,t 使①,②式均成立.

则由①+②得:$2z^2=t^2+x^2$ ③

因而 x 与 t 的奇偶性相同.将③式变形为

$$z^2=\left(\frac{x+t}{2}\right)^2+\left(\frac{x-t}{2}\right)^2 \quad ④$$

不妨设 x 与 t 互质(否则由①,③两式可以推知 y,z 均能被 (x,t) 整除,则考察 $\frac{x}{(x,t)}$,$\frac{y}{(x,t)}$,$\frac{z}{(x,t)}$,$\frac{t}{(x,t)}$ 即可),则 $\left(\frac{x+t}{2},\frac{x-t}{2}\right)=1$,于是由勾股数的知识知存在 $m,n\in\mathbf{N}_+$,$(m,n)=1$,m,n 一奇一偶,使得 $\frac{x+t}{2}\cdot\frac{-x+t}{2}=2mn(m^2-n^2)$ ⑤

于是由①-②得:$y^2=\frac{1}{2}(t^2-x^2)=4mn(m+n)(m-n)$ ⑥

⑥式中的 $m,n,m+n,m-n$ 两两互质,所以存在 $a,b,c,d\in\mathbf{N}_+$,使得

$m=a^2,n=b^2,m+n=c^2,m-n=d^2$.

即有 $\begin{cases}a^2+b^2=c^2,\\a^2-b^2=d^2.\end{cases}$

显然有 $a\leqslant m<y<z$,则由原方程的一组正整数解 (x,y,z,t) 可以得出一组新数组 (d,b,a,c) 且 $a\leqslant z-1$,则由无穷递降法即可以得出矛盾.

所以方程组①,②没有正整数解.

6. 提示:我们先可假设 $(x,z)=1$,进而可以得知 x,y,z 两两互质,易知 z 必为奇数.如果 x 为偶数,则由勾股数的知识知存在 $a,b\in\mathbf{N}_+$,有 $x^2=a^2-b^2,z^2=a^2+b^2$,再利用习题5的结论便可得出矛盾.如果 x 为奇数,则存在 $\alpha,\beta\in\mathbf{N}_+$,使得 $z^2=a^2+b^2,x^2=2ab$,于是 $x^2+z^2=(a+b)^2,z^2-x^2=(a-b)^2$,再利用习题5的结论即可.

7. 证明:设 (x_0,y_0) 是方程 $x^2+y^2-19xy-19=0$ (*)

的一组整数解,则显然 $x_0\neq0,y_0\neq0$,并且 $19(x_0y_0+1)=x_0^2+y_0^2>0$.

由此即知 $x_0y_0\geqslant0$,x_0,y_0 必须同号.

不妨设 x_0,y_0 均为正整数(否则分别用 $-x_0,-y_0$ 代替 x_0,y_0),并且 $x_0\geqslant y_0$.

将(*)式看做关于 x 的一元二次方程:

$x^2-19y_0\cdot x+(y_0^2-19)=0$ ①

则 x_0 是①的解,那么由韦达定理知①的另一个实根为:$x'=19y_0-x_0$.

由于 $x_0,y_0\in\mathbf{N}_+$,所以 $x'\in\mathbf{Z}$,由于 x' 使①成立,所以 (x',y_0) 使(*)成立,则易知 x' 与 y_0 同号,即 $x'\in\mathbf{N}_+$.

又由韦达定理知:$x'=\frac{y_0^2-19}{x_0}<\frac{y_0^2}{x_0}\leqslant y_0\leqslant x_0$.

所以由(*)的一组正整数解$(x_0,y_0)(x_0\geqslant y_0)$，可导出它的另一组正整数解$(y,x')$ $(y\geqslant x')$，并且$y+x'<x+y$.

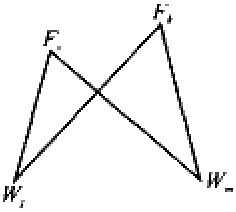
将这一过程无限地进行下去，每次新得出的一组解中两数之和都严格地小于前一组解中两数之和，而这些解都为正整数解，这显然是不可能的.

所以原不定方程没有整数解.

§6.2　无穷递降法的其他应用

1. 解：假设$\sqrt{5}$不是无理数，那么存在正整数a,b使得$\frac{b}{a}=\sqrt{5}$，即$b^2=5a^2$，由此易知b是5的倍数，设$b_1=\frac{b}{5}$，则有$(5b_1)^2=5a^2(b\in \mathbf{N}_+)$，所以$a^2=5b_1^2$，由此又可得知$a$是5的倍数，设$a_1=\frac{a}{5}(a_1\in \mathbf{N}_+)$，则有$(5a_1)^2=5b_1^2$，所以$b_1^2=5a_1^2$，于是我又找到了$(b_1,a_1)(a_1,b_1\in \mathbf{N}_+)$，使得$b_1^2=5a_1^2$并且$b_1+a_1<a+b$. 将上述过程无限地进行下去，就可以得出矛盾. 由此可以得知$\sqrt{5}$是无理数.

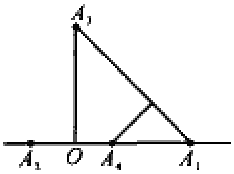
2. 证明：对于任意一种分配方法，如果存在两条公路F_iW_m和F_kW_j相交(如第2题图)，其中$1\leqslant i,k\leqslant n,1\leqslant j,m\leqslant n$且$i\neq k,j\neq m$.



第2题图

在这种情况下，我们作如下调整：去掉公路F_iW_m和F_kW_j，改为F_kW_m和F_iW_j. 此时有$F_iW_m+F_kW_j>F_iW_j+F_kW_m$(由于$F_1,F_2,\cdots,F_n,W_1,W_2,\cdots,W_n$中无三点共线，故此处必为严格的大于号)如果调整后仍有某两条公路相交，则再作出如同上述的调整，每经过一次调整，n条公路的总长度都严格减小，而公路的分配方式共有$n!$种(有限种)，故上述递降过程不可能无限地进行下去，必在某一次调整后停止，那么，此时所得的分配方式中，n条公路两两之间都没有交点.

3. 证明：设$M=\{A_1,A_2,\cdots,A_n\}$. 假设$A_1,A_2,\cdots,A_n$不全共线，则对任意的$A_i,A_j\in M,i\neq j$，存在$A_k\in M$，使A_i,A_j,A_k三点不共线$(k\neq i,k\neq j)$. 定义集合$D=\{$点A_i到线段A_jA_k的距离$|1\leqslant i,j,k\leqslant n$，$i,j,k$两两不等，$A_i,A_j,A_k$三点不共线$\}$，任取直线$A_iA_j$，不妨$i\neq j$. 此时必存在$M$中的某个点不在$A_1A_2$上，不妨设这点为$A_3$，如第3题图，设$A_3O\perp A_1A_2$，依题意知在$\{A_4,A_5,A_6,\cdots,A_n\}$中必存在某点在直线$A_1A_2$上，不妨设该点为$A_4$，且$A_1,A_4$在直线$A_3O$同侧，不妨$A_4$在线段$OA_1$上(包括端点)，则$A_4$到直线$A_1A_3$的距离不小于点$O$到直线$A_1A_3$的距离，小于$A_3$到直线$A_1A_2$的距离(即为$A_3O$). 由此我们由一个"点线组"$(A_3,A_2A_4)$得到一个新"点线组"$(A_4,A_1A_3)$并且$d(A_3,A_2A_4)>d(A_4,A_1A_3)$(其中$d(A_i,A_jA_k)$表示点$A_i$到直线$A_jA_k$的距离，$A_i$不在线段$A_jA_k$上). 反复进行如上操作，可不断地得到新"点线组"，其中"点"

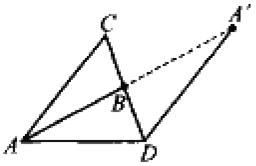


第3题图

到“线”的距离不断地减小且大于 0). 由此可以得知 D 中有无穷多个元素，而事实上 D 中元素个数 $\leqslant nC_{n-1}^{2}$，矛盾. 所以，M 中的所有点共线.

4. 证明：用反证法证明. 假设集合 M 是有限点集.

在点集 M 中任取两点 A，B，依题意知存在线段 CD，使点 B 为线段 CD 的中点(其中 C，$D\in M$)如第 4 题图.



第 4 题图

若 C 在直线 AB 上，则 D 也在直线 AB 上且 C，D 中至少有一点与 A 位于直线 AB 上点 B 的异侧，不妨点 D 与 A 位于点 B 异侧，则有 $AD>AB$，由此，在这种情况下，我们便找到一条以 M 中的点为端点，且长度比 AB 更大的线段.

若 C，D 不在直线 AB 上，则延长 AB 至 A'，使 $AB=BA'$，连结 $A'D$，则 $A'D=AC$.

从而 $AC+AD=A'D+AD>A'A=2AB$.

则 AC，AD 中至少有一个大于 AB，即在这种情况下，我们同样找到了一条以 M 中的点为端点且长度比 AB 更大的线段.

综合以上两方面，知无论哪种情形，我们都可以找到一条线段 AD 比 AB 更长(A，B，$D\in M$). 反复进行上述过程，我们可以不断地找出更长的线段且这些线段的端点都为 M 中的点，而以 M 中的点为端点的线段只有有限条，这就导致了矛盾.

所以 M 必为无限点集.

(本题中，通过“无穷递增”来得出矛盾. 事实上，我们也可以将上述过程看作为所得新线段与以 M 中的点为端点的线段中最长者的距离不断地减小).

5. 证明：根据题设，我们可以得知 $\sum\limits_{i\neq k}a_i$ $(k=1,2,3,\cdots,2n)$ 必为偶数.

由此可知对任意 $k\in\{1,2,3,\cdots,2n\}$，$\sum\limits_{i=1}^{2n}a_i$ 与 a_k 同奇偶.

显然 a_1，a_2，$\cdots$，a_{2n} 应同为偶数(否则，a_1，a_2，$\cdots$，a_{2n} 必同为奇数，但此时 $\sum\limits_{i=1}^{2n}a_i$ 为偶数，这与前面的结论矛盾).

这样一来，$\frac{a_1}{2}$，$\frac{a_2}{2}$，$\cdots$，$\frac{a_{2n}}{2}$ 都是整数，且仍满足题中所述性质.

同前面的方法可以证明 $\frac{a_1}{2^2}$，$\frac{a_2}{2^2}$，$\cdots$，$\frac{a_{2n}}{2^2}$ 都是整数；$\frac{a_1}{2^3}$，$\frac{a_2}{2^3}$，$\cdots$，$\frac{a_{2n}}{2^3}$ 都是整数……

重复上述讨论可知，对任一正整数 m，恒有 $\frac{a_1}{2^m}$，$\frac{a_2}{2^m}$，$\cdots$，$\frac{a_{2n}}{2^m}$ 都是整数.

由此就可以得知，$a_1=a_2=\cdots=a_{2n}=0$.

6. 证明：首先给出一个引理

引理：方程组 $\begin{cases}x^2+y^2=z^2,\\x^2-y^2=w^2\end{cases}$ 没有正整数解.

引理证明略(参见第六章第1节习题5).

下面证明原命题:

用反证法,假设存在面积为平方数的勾股三角形.

设这样的一个三角形的三边长分别为 a,b,c.(其中 a,b 为这个三角形的两条直角边长,c 为斜边长),则有

$a^2+b^2=c^2$ 且 $\frac{1}{2}ab$ 为平方数.

由勾股数知识知存在 $u,v\in\mathbf{N}_+$ 使得 $c=u^2+v^2$,且不妨设 $a=u^2-v^2,b=2uv$(我们可以不妨 a,b,c 两两互质,则可以得到这些式子,并且 $(u,v)=1$ 且 u 与 v 互质).

则该勾股三角形面积为 $uv(u^2-v^2)$,即 $uv(u-v)(u+v)$ 为平方数.

由于 u,v 互质且 u,v 一奇一偶,所以 $u,v,u+v,u-v$ 两两互质.

进而知 $u,v,u+v,u-v$ 都为完全平方数.

设 $u=s^2,v=t^2,u+v=p^2,u-v=q^2$(其中 $s,t,p,q\in\mathbf{N}_+$).

则有如下两式 $\begin{cases}s^2+t^2=p^2,\\ s^2-t^2=q^2.\end{cases}$

利用引理便得出矛盾.所以不存在面积为平方数的勾股三角形.

第七章　格点及其性质

§7.1　格点的定义及其分类

1. B　考虑以 $A(0,0),B(0,1),C(1,1),D(1,0)$ 为顶点的正方形 $ABCD$,其内部不存在格点,故所求的 $n\geqslant5$.

另一方面,根据格点的奇偶性分类,可以分为如下四类:(奇,奇),(奇,偶),(偶,奇),(偶,偶),凸五边形的五个顶点中必有两个属于同一类,则这两个顶点的中点也是格点,且这个格点在凸五边形的内部,故所求的 $n\leqslant5$.

2. D　对任意 $m\in\mathbf{Z}$,直线 $m(2y-1)=x-10$ 经过点 $\left(10,\frac{1}{2}\right)$,还经过格点 $(10+m(2t-1),t)(t\in\mathbf{Z})$.故由 m 的任意性知,所求的直线有无穷多条.

3. A　由点到直线的距离公式知,格点 $P(x,y)$ 到直线 l 的距离 $d=\frac{|5(3y-5x)-12|}{5\sqrt{34}}$.

而 $x,y\in\mathbf{Z}$,所以 $|5(3y-5x)-12|$ 的最小值等于2,故 d 的最小值等于 $\frac{2}{5\sqrt{34}}=\frac{\sqrt{34}}{85}$.

4. B　圆 C 方程为:$(x-\sqrt{2})^2+(y-\sqrt{3})^2=r^2$.

如果圆 C 上有两个格点 $A(x_1,y_1)$ 和 $B(x_2,y_2)$，则 $(x_1-\sqrt{2})^2+(y_1-\sqrt{3})^2=r^2$，$(x_2-\sqrt{2})^2+(y_2-\sqrt{3})^2=r^2$.

以上两式相减得 $2\sqrt{2}(x_2-x_1)+2\sqrt{3}(y_2-y_1)+(x_1^2+y_1^2)-(x_2^2+y_2^2)=0$.

而 $x_1=x_2$，$y_1=y_2$ 不可能同时成立. 所以 $2\sqrt{2}(x_2-x_1)+2\sqrt{3}(y_2-y_1)\notin\mathbf{Q}$（$\mathbf{Q}$ 为有理数集）这与上面的式子相违，故圆 C 至多经过一个格点.

又因为当 $r=\sqrt{5}$ 时，圆 C 经过原点，所以圆 C 最多经过一个格点.

5. (44,19)　因为区域 $0\leqslant x\leqslant k$，$0\leqslant y\leqslant k$ 内的格点个数 $(k+1)^2$，又 $44^2=1936<2006$，$45^2=2025>2006$，所以编号为 2006 的点的横坐标是 44 或纵坐标是 44，因为 44 为偶数，所以应由点 (0,44) 向右数，又因 $2006-44^2=70>44$，所以编号为 2006 的点的横坐标为 44，纵坐标为 $44-(70-45)=19$. 即编号为 2006 的点的坐标为 (44,19).

6. 16　由于 $(|x|-1)^2\leqslant(|x|-1)^2+(|y|-1)^2<2$.

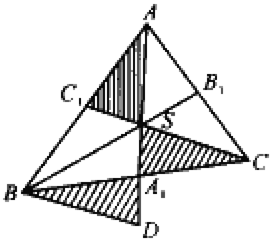
所以 $(|x|-1)^2<2$，$-1\leqslant|x|-1\leqslant1$，即 $0\leqslant|x|\leqslant2$，同理 $0\leqslant|y|\leqslant2$.

经检验 $(x,y)=(-1,\pm1),(-1,0),(1,0),(0,\pm1),(-1,\pm2),(1,\pm2),(-2,\pm1),(2,\pm1)$ 是满足原不等式的 16 个整数解.

7. 7　由已知，A 表示以点 (3,4) 为圆心，$\frac{5}{2}$ 为半径的圆及其内部，而 B 表示以 (4,5) 为圆心，$\frac{5}{2}$ 为半径的圆外部，其中有 7 个点 (1,3)，(1,4)，(1,5)，(2,3)，(2,2)，(3,2)，(4,2).

8. 证明：设 $p(x,y)$ 为整点，则与之相邻的四个点是 $(x\pm1,y)$，$(x,y\pm1)$，构造函数 $f(x,y)=x+2y$，则 p 与其相邻的点对应 5 个不同的值：$x+2y$，$x+2y\pm1$，$x+2y\pm2$，这是 5 个相邻的整数，其中有且仅有一个能被 5 整除，于是令 $s=\{(x,y)\mid x\in\mathbf{Z},y\in\mathbf{Z},5\mid x+2y\}$，则 s 即为所求.

9. 证明：设整点 $\triangle ABC$ 是符合题意的三角形.



第 9 题图

$\triangle ABC$ 的三条中线 AA_1，BB_1，CC_1 把这个三角形分成 6 个三角形.

位于 $\triangle ABC$ 内的唯一整点 T 至少属于这六个三角形中的某一个，不妨设 T 在 $\triangle AC_1S$ 的内部或边界上，但不在边 AC_1 上.

以顶点 A 为位似中心，位似系数等于 2，对 $\triangle AC_1S$ 作位似变换得到 $\triangle ABD$，则整点 T 变换成新的整点 T'，T' 在 $\triangle ABD$ 的内部或边界上，但不在边 AB 上.

因为在 $\triangle ABC$ 内只有一个整点 T，则 T' 只能在 $\triangle A_1BD$ 的内部或边界上，但不和 B 点重合.

注意到 $BA_1=A_1C, SA_1=A_1D$，所以$\triangle A_1BD$与$\triangle A_1CS$关于A_1对称，于是T'关于A_1的对称点也是整点，并且在$\triangle A_1CS$的内部或边界上，但不与C重合，由于在$\triangle ABC$内只有一个整点，于是在$\triangle AC_1S$与$\triangle A_1CS$内部或边界上的这两个整点应为同一个整点，这个整点只能在$\triangle AC_1S$与$\triangle A_1CS$的公共顶点S处，即T与$\triangle ABC$的重心S重合(本题还可以用下一节的格点多边形的面积计算定理证明).

10. 考虑格点$(i,i^2)(i\in \mathbf{N})$，这样的格点显然有无穷多个，它们都在抛物线$y=x^2(x\geqslant 0)$上，其中任三点都不共线，从这些点中任取两点$M_i(i,i^2)$，$M_j(j,j^2)$，则$|M_iM_j|=\sqrt{(i-j)^2+(i^2-j^2)^2}=|i-j|\cdot\sqrt{(i+j)^2+1}$，而$i+j\geqslant 1$，则$(i+j)^2+1$不是完全平方数，则$|M_iM_j|$一定不是有理数.

§7.2 格点的计数

1. C 设三角形三边长为整数x,y,z，且$x\leqslant y\leqslant z$，则$z=11$，$x+y\geqslant 12$，$x\leqslant y\leqslant 11$.

因此，只需求出由直线$y=12-x$，$y=11$，$y=x$围成的三角形(含边界)内的整点个数即可，容易算得所求整点个数是36个.

2. C 满足题意的整点是由直线$y=-x+8$，$y=x-1$，$y=9$围成的三角形区域内(不含边界)，当$x=k(1\leqslant k\leqslant 4)$时，$9-k\leqslant y\leqslant 8$，$y$可取$8-(9-k)+1=k$种值.

当$x=k(5\leqslant k\leqslant 8)$时，$k\leqslant y\leqslant 8$，$y$有$9-k$种值.

因此所求整点个数为$\sum\limits_{k=1}^{4}k+\sum\limits_{k=5}^{8}(9-k)=20$.

3. B 设(x,y)是已知的圆上的整点，则$(x-199)^2+y^2=199^2$.

显然$(x,y)=(0,0),(199,199),(199,-199),(398,0)$为方程4个解.

当$y\neq 0$且$y\neq\pm 199$时，y与199互素(因199为质数)，此时$199,y,|199-x|$是一组勾股数，故199可表成二个正整数的平方和，即$199=m^2+n^2$.

因$199=4\times 49+3$，可设$m=2k$，$n=2l+1$，$k\in\mathbf{Z}$，$l\in\mathbf{Z}$.

则$199=4k^2+4l^2+4l+1=4(k^2+l^2+l)+1$.

这与199为$4d+3$型素数矛盾，因而圆O上只有四个整点：$(0,0),(199,\pm 199),(398,0)$.

4. 9801 点(x,y)在该$\triangle OAB$内当且仅当$y<2x$，$y>0$，$x<100$且$x>0$，对$x=k(1\leqslant k\leqslant 99)$，$y$可取$1,2,\cdots,2k-1$，故$\triangle OAB$内共有整点$\sum\limits_{k=1}^{99}(2k-1)=99^2=9801$.

5. 10011 由$\dfrac{x^2+y^2}{7}\in\mathbf{Z}$知$7|x^2+y^2$.

当$7|x$且$7|y$时，显然有$7|x^2+y^2$.

当$7\nmid x$或$7\nmid y$时，由$7|x^2+y^2$知，$7\nmid x$且$7\nmid y$. 由费尔马小定理$x^6\equiv 1(\mathrm{mod}7)$，即$(x^2)^3\equiv 1(\mathrm{mod}7)$，又$x^2\equiv -y^2(\mathrm{mod}7)$，所以$(-y^2)^3\equiv 1(\mathrm{mod}7)$，即$-y^6\equiv 1(\mathrm{mod}7)$，又由

费尔马小定理，$y^6\equiv1 \pmod 7$，这与 $-y^6\equiv1 \pmod 7$ 矛盾.

综上，$\frac{x^2+y^2}{7}\in\mathbf{Z}(x,y\in\mathbf{Z})\Leftrightarrow7\mid x,7\mid y$.

故所求的整数对 (x,y) 有 $C_{142}^2=10011$ 个.

6. 202　令 $T_1=\left\{(x,y)\mid 0<x\leqslant\sqrt{48},0<y\leqslant\frac{n}{x}\right\}$,

$T_2=\left\{(x,y)\mid 0<y\leqslant\sqrt{48},0<x\leqslant\frac{n}{y}\right\}$.

则 $T=T_1\cup T_2$，$T_1\cap T_2=\{(x,y)\mid 0<x\leqslant\sqrt{48},0<y<\sqrt{48}\}$，用 $\|x\|$ 表示集 x 内格点的个数，于是根据容斥原理，有

$$\begin{aligned}\|T\|&=\|T_1\cup T_2\|\\&=\|T_1\|+\|T_2\|-\|T_1\cap T_2\|\\&=\sum_{0<x\leqslant\sqrt{48}}\left[\frac{48}{x}\right]+\sum_{0<y\leqslant\sqrt{48}}\left[\frac{48}{y}\right]-[\sqrt{48}]^2\\&=2\sum_{0<k\leqslant6}\left[\frac{48}{k}\right]-36=119\times2-36=202.\end{aligned}$$

7. 设此三角形三边长为 $x,y,z(x\leqslant y\leqslant z)$.

由题意得 $0<x\leqslant y\leqslant z<100,x+z=2y,x+y>z$.

消去 z 得 $0\leqslant x<y<\frac{x}{2}+50,y<2x$. 作出满足上述不等式组的平面区域，显然平面区域内整点的个数就是要求的三角形的个数，用直线 $x=k(1\leqslant k\leqslant99$，且 $k\in\mathbf{N})$ 去切割平面区域，有：

(1) 当 $1\leqslant k\leqslant33$ 时，直线 $x=k$ 上的整点有 $(k,k),(k,k+1)\cdots,(k,2k-1)$，共 k 个，这里满足题意的整点有 $\sum\limits_{k=1}^{33}k=561$ 个；

(2) 当 $34\leqslant k\leqslant99$ 时，当 k 为偶数，直线 $x=k$ 上的整点有 $(k,k),(k,k+1),\cdots,\left(k,\frac{k}{2}+50-1\right)$，共 $50-\frac{k}{2}$ 个；

当 k 为奇数，直线 $x=k$ 上的整点有 $(k,k),(k,k+1),\cdots,\left(k,\frac{k-1}{2}+50\right)$，共 $50-\frac{k-1}{2}$ 个.

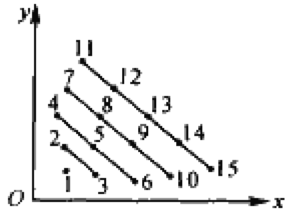
所以 $34\leqslant k\leqslant99$ 内整点个数为 $2(33+32+\cdots+1)=1122$ 个.

综合(1)与(2)，满足题意的三角形有 $561+1122=1683$ 个.

8. 证明：记 $B(0,b)$，其中 $b=2p_1p_2\cdots p_{2008}$.（p_i 为不同因子，$i=1,2,\cdots,2008$），记 $A_j(a_j,0)$，其中 $a_j=|(p_1p_2\cdots p_j)^2-(p_{j+1}p_{j+2}\cdots p_{2008})^2|$，$j=1,2,\cdots,2007$.

由勾股数组公式易知$|A_jB|=\sqrt{b^2+a_j^2}\in \mathbf{N}_+$，又$|A_iA_j|=|a_j-a_i|(1\leqslant i<j\leqslant 2007)$是个整数，即以上找到的 2008 个格点 $B,A_j(j=1,2,\cdots,2007)$不全在一条直线上，且两两之间的距离均为整数.

9. 证明：对坐标平面内第一象限内的格点(x,y)，当 $x+y$ 的值相同时，它们处于同一条斜线上(如图所示).



第 9 题图

$1\leftrightarrow(1,1)$；$2\leftrightarrow(1,2)$，$3\leftrightarrow(2,1)$；$4\leftrightarrow(1,3)$，$5\leftrightarrow(2,2)$，$6\leftrightarrow(3,1)$；$7\leftrightarrow(1,4)$，$8\leftrightarrow(2,3)$，$9\leftrightarrow(3,2)$，$10\leftrightarrow(4,1)$；……

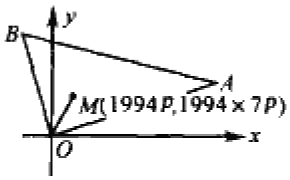
这样第一象限的格点与正整数对可建立一一对应.

由于各条斜线上的格点的个数为 $1,2,3,4,\cdots,n,\cdots$ 而各条斜线上的格点(x,y)的 $x+y$ 的值分别是 $2,3,4,\cdots,n+1,\cdots$. 一方面，对任意的 $a\in\mathbf{N}_+$，有且只有一个格点(x_0,y_0)的序号是 a. 另一方面，格点(x_0,y_0)位于第 x_0+y_0-1 条斜线上，它的前面有 x_0+y_0-2 条斜线，故共有格点 $1+2+3+\cdots+(x_0+y_0-2)=\frac{1}{2}(x_0+y_0-1)(x_0+y_0-2)$个. 而这点处在 x_0+y_0-1 条斜线的第 x_0 个位置上，所以它的序号应是 $x_0+\frac{1}{2}(x_0+y_0-1)(x_0+y_0-2)$.

由于同一格点的序号是唯一确定的，所以 $x_0+\frac{1}{2}(x_0+y_0-1)(x_0+y_0-2)=a$，即$(x_0,y_0)$是原方程的正整数解，而且是惟一的.

10. 解：连坐标原点 O 及点 M，取线段 OM 的中点 $I(P\times 997,7P\times 997)$，把满足条件的一个直角三角形关于点 I 作一个中心对称变换，即把点(x,y)变为点$(P\times 1994-x,7P\times 1994-y)$，于是，满足题目条件的一个整点三角形变为一个与之全等的整点直角三角形，三角形的内心变到点 M，直角顶点变为坐标原点，因此，所求整点直角三角形的个数，只需考虑直角顶点在坐标原点，内心在点 M 的情况即可.

考虑满足上述条件的整点 $\mathrm{Rt}\triangle OAB$(如图所示). 设$\angle xOM=\beta$，$\angle xOA=\alpha$，$\alpha+\frac{\pi}{4}=\beta$. 由题目条件，$\tan\beta=7$，$\tan\alpha=\tan\left(\beta-\frac{\pi}{4}\right)=\frac{\tan\beta-1}{1+\tan\beta}=\frac{3}{4}$. 于是直角边 OA 上的任一点的坐标可写成$(4t,3t)$，由于 A 是整点，故可设 $A(4t,3t)(t\in\mathbf{N}_+)$，则$|OA|=5t$，从$\angle yOB=\alpha$，可设 B 的坐标为$(-3t',4t')(t\in\mathbf{N}_+)$，则$|OB|=5t'$，直角三角形的内切圆半径 $r=\frac{\sqrt{2}}{2}|OM|=5p\times 1994$.



第 10 题图

设$|OA|=2r+p'$，$OB=2r+q'$，由于$|OA|$，$|OB|$，r 皆为 5 的倍数，则正整数 p' 和 q' 都是 5 的倍数，利用圆外一点到圆的两条切线长相等，有$|AB|=(r+p')+(r+q')=2r$

$+p'+q'$.

由于△是一个直角三角形，有

$0=AB^2-OA^2-OB^2=(2r+p'+q')^2-(2r+p)^2-(2r+q)^2=2p'q'-4r^2$

可得 $p'q'=r^2$.

由 $\frac{p'}{5},\frac{q'}{5}\in\mathbf{N}_+$，可得 $\frac{p'}{5}\cdot\frac{q'}{5}=2^3\times997^2\times p^2$.

当 $p\neq2$ 且 $p\neq997$ 时，有 $\frac{p'}{5}=2^i\times997^j\times p^k$，$\frac{q'}{5}=2^{3-i}\times997^{2-j}\times p^{2-k}$，这里 $i=0,1,2,3$；$j=0,1,2$；$k=0,1,2$. 那么 $\left(\frac{p'}{5},\frac{q'}{5}\right)$ 有 $4\times3\times3=36$ 组不同的(有序)解. 同理，当 $p=2$ 时，$\left(\frac{p'}{5},\frac{q'}{5}\right)$ 有 $6\times3=18$ 组不同的(有序)解. 当 $p=997$ 时，方程组有 $4\times5=20$ 组不同的(有序)解.

于是，所求的直角三角形的个数

$$S=\begin{cases}36 & \text{当 } p\neq2 \text{ 且 } p\neq997 \text{ 时},\\ 18 & \text{当 } p=2 \text{ 时},\\ 20 & \text{当 } p=997 \text{ 时}.\end{cases}$$

§7.3 格点的染色、覆盖及其他

1. 由格点多边形的面积计算定理，多边形的面积 $S\geqslant\frac{1}{2}\times3+2-1=\frac{5}{2}$.

另一方面，取点 $A(0,0)$，$B(1,4)$和 $C(2,3)$，则△ABC 内有两个格点，且△ABC 的面积等于$\frac{5}{2}$. 故所求的面积的最小值为$\frac{5}{2}$.

2. 证明：假设存在格点凸五边形，其内部不含格点，因格点凸多边形的面积的两倍是整数，故存在一个面积最小且其内部不含格点的整点凸五边形，不妨设为 $ABCDE$.

又根据整点的奇偶性，可将整点分为四类：(奇，奇)，(奇，偶)，(偶，奇)，(偶，偶)，则 A，B，C，D，E 中有两点属于同一类，不妨其中有一个点是 A，如果另一点是 D 或 E，不妨设为 D，则 AD 中点为格点，且它在五边形内部，矛盾.

如果另一点是 B 或 C，不妨设为 B，则 AB 中点 M 也为格点，则凸五边形 $BCDEM$ 是格点凸五边形，且它的内部不含格点，其面积也小于 $ABCDE$ 的面积，这与 $ABCDE$ 面积的最小性矛盾.

所以假设不成立，故所有的格点凸五边形内部都存在一个格点.

3. 证明：取一个方格纸上的结点为原点建立直角坐标系，使得方格纸上所有的结点均为格点.

于是闭折线的每个顶点$(x_i,y_i)(i=1,2,\cdots,n)$的横、纵坐标均为整数.

因为是闭折线，则闭折线在坐标轴上的投影(连同符号)满足 $x_1+x_2+\cdots+x_n=0$，$y_1+y_2+\cdots+y_n=0$，$x_i^2+y_i^2=c(i=1,2,\cdots,n)$.

(1)若 c 具有 $4k+2$ 的形式.

这时，x_i 和 y_i 恒为奇数，而由于 n 个奇数的和为 0，故知 n 为偶数.

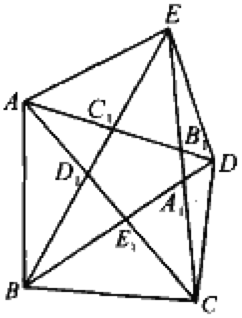
(2)若 c 具有 $4k+1$ 的形式.

这时，x_i 与 y_i 的奇偶性不同，即 x_i+y_i 是奇数，又 $(x_1+y_1)+(x_2+y_2)+\cdots+(x_n+y_n)=0$. 所以 n 为偶数.

(3)若 c 具有 $4k$ 的形式.

这时，x_i 和 y_i 是偶数，设 2^k 是所有 x_i 和 y_i 都可被其整除的 2 的最高方幂，这时在 $x_i^2+y_i^2=c(i=1,2,\cdots,n)$ 的两边，同时除以 2^k，就可化为 x_i 与 y_i 要么同为奇数，或为一奇一偶的情形，即情形(1)，(2)，此时 n 亦为偶数.

综上，n 为偶数.



4. 为了说话方便，将"在内部或在周界上"统称为"在…中"，用反证法，假设结论不成立. 我们考虑结论不成立的具有最小面积 S 的凸五边形 $ABCDE$，并称图中 $A_1B_1C_1D_1E_1$ 为 $ABCDE$ 的"内"五边形，首先证明 $\triangle AC_1D_1$ 中的所有整点，除 A_1 外，只可能在 C_1D_1 上. 事实上，如果在 $\triangle AC_1D_1$ 中除 A 外，还有整点 K 不在 C_1D_1 上，那么凸五边形 $KBCDE$ 的"内"五边形在 $A_1B_1C_1D_1E_1$ 中便没有格点，这和 S 的最小性矛盾.

从 $\triangle ABC$，$\triangle BCD$，$\triangle CDE$，$\triangle DEA$，$\triangle EAB$ 中选出面积最小的一个，设为 $\triangle ABC$. 于是 A 到 BC 的距离不大于 D 到 BC 的距离，C 到 AB 的距离不大于 E 到 AB 的距离，考察使 $ABCO$ 为平行四边形的点 O，则 O 位于 $\triangle AB_1C$ 之中，且由 A,B,C 为整点知 O 为整点，而且前面的证明知 O 不在 $\triangle AC_1D_1$ 内部，也不在 $\triangle CA_1E_1$ 内部，即知 O 在 $A_1B_1C_1D_1E_1$ 中，这与假设矛盾.

5. 证明：将 $T_1=\{(x,y)\mid x,y\in\mathbf{Z},|x|\geqslant|y|\}$ 中的点染成红色，将 $T_2=\{(x,y)\mid x,y\in\mathbf{Z},|x|<|y|\}$ 中的点染成蓝色，则将平面上所有格点都染成红、蓝两色之一.

对于任意平行于 y 轴的直线 $x=t(t\in\mathbf{R})$，若 $t\notin\mathbf{Z}$，则此直线上不含任何红点.

若 $t\in\mathbf{Z}$，则此直线上的红点形如 (t,y)，(这里 y 是绝对值不大于 t 的整数)，故此直线上红点仅有有限多个.

同理，任一平行于 x 轴的直线上仅有有限多个蓝点.